CHAPTER 1

Admission Control for the Cisco Cable Modem Termination System

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

Admission Control for the Cisco Cable Modem Termination System (CMTS) is a multifaceted feature that implements a Quality of Service (QoS) policy on the CMTS Headend. Admission Control establishes efficient resource and bandwidth utilization in a way that was not possible in prior Cisco IOS releases.

Admission Control monitors multiple system-level resources on the Cisco CMTS, and performs automatic resource allocation on a service-request basis. Admission Control maintains optimal system-level operation by preventing resource consumption that would otherwise degrade the performance for the entire Cisco CMTS. Furthermore, Admission Control can allocate upstream or downstream bandwidth resources to specific DOCSIS traffic types, and maintain such prioritization amidst very dynamic traffic conditions.

When any system-level or bandwidth-level resource approaches critical consumption levels, Admission Control implements graceful degradation of service in a planned and graceful manner. Admission Control supports multiple new commands for traffic and resource monitoring. This document describes the principles, configuration, operation and other information about Admission Control on the Cisco CMTS for Cisco IOS Release 12.3(13a)BCBC.

Feature History for Admission Control for the Cisco CMTS

Release	Modification
12.3(13a)BC	This feature was introduced on the Cisco uBR10012 and the Cisco uBR7246VXR universal broadband routers.

Note *Admission Control* is a widely used term that applies to similarly named features for many additional Cisco products and technologies. One distinct version of Admission Control is supported for the Cisco uBR7114 universal broadband router in Cisco IOS 12.1 EC software.

This prior Admission Control feature sets the percentage of upstream channel capacity allowable for the given upstream. Refer to the *Cisco uBR7100 Series Software Configuration Guide* for additional information in this case:

- http://www.cisco.com/en/US/docs/cable/cmts/ubr7100/configuration/guide/scg7100.html

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp 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 Admission Control for the Cisco CMTS

Admission Control on the Cisco CMTS requires Cisco IOS Release 12.3(13a)BCBC or later, with these additional provisions.

Cisco uBR10012 Router

- Performance routing engine 1 or 2 (PRE1 or PRE2) modules must be installed and operational on the Cisco uBR10012 router.
- Cisco uBR10-MC5X20U Broadband Processing Engines (BPEs) must be installed and operational on the Cisco uBR10012 router.

Cisco uBR7246VXR Router

- Cisco uBR-MC28U broadband processing engine (BPE) or Cisco MC16/MC28 cable interface line cards must be installed and operational on the Cisco uBR7246VXR router.

Restrictions for Admission Control on the Cisco CMTS

General Restriction

The Admission Control feature is not designed to change thresholds in irregular or spontaneous fashion. For example, if voice calls are already in progress, and you attempt to configure thresholds for voice, the bandwidth usage of the existing calls may not be accounted in accurate fashion. This example results in inaccurately enforcing the Admission Control policy on the desired interface.

As a workaround, configure Admission Control 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.

Further Restrictions

Admission Control in Cisco IOS Release 12.3(13a)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)

Future Cisco IOS releases will enhance resources with Admission Control on the Cisco CMTS.

Admission Control in Cisco IOS Release 12.3(13a)BC has the following general restrictions:

- Admission Control does not support Wide Area Network (WAN) bandwidth monitoring for the Cisco uBR10012 router.

Caveats

Open Caveats for Admission Control in Cisco IOS Release 12.3(13a)BCBC

Table 1-1 Open Caveats for Admission Control in Cisco IOS Release 12.3(13a)BCBC

DDTS ID Number	Description
Refer to release notes.	**US reservation value increments differently on identical voice calls** This apparent difference may arise because the values are printed to 1% accuracy. Fractions of 1% are not printed. Therefore, the actual value of 4.6% is printed as 4%, and the value 5.2% is printed as 5%, for example. This can give the impression that first call consumed 4% of bandwidth, but the second call consumed 5%, and this exaggerates the apparent difference.
Refer to release notes.	**Service class sched type is incorrect with service class name** If the scheduling type for a given service class name is different in the CM configuration file and the router configuration, the type from the router configuration will take precedence.

Table 1-1 Open Caveats for Admission Control in Cisco IOS Release 12.3(13a)BCBC

DDTS ID Number	Description
Refer to release notes.	**Inconsistency in threshold counter during a voice call** Admission Control checks are performed each time DSA or DSC requests are made. For the same voice call, the MTA device may send several DSC request messages. Some of these messages may not request additional bandwidth. Even if new bandwidth is not requested, and the current utilization is above major or minor threshold, an alarm is generated, and the counter is incremented.
CSCsb27203	**Validation Checks** Admission Control validates bandwidth threshold with validation checks, but only for the traffic types for which this feature is configured. Otherwise, Admission Control does not validate resource configurations on the Cisco CMTS. For example, if you configure downstream (DS) bandwidth Admission Control for CIR data at 40% exclusive threshold, this implicitly limits the voice usage to 60% of the total configurable bandwidth. In this example, voice thresholds are configured so that the sum of exclusive and non-exclusive thresholds is less than 60% of the total resource available. Furthermore, in this example, the voice usage may exceed the implicit limit of 60% bandwidth, and occupy the 40% bandwidth reserved exclusively for data. To avoid this problem, configure Admission Control for all the traffic types in a given direction (US or DS). If you do not set Admission Control thresholds for voice, the voice Admission Control check is not performed. Therefore, the new calls are accepted without Admission Control checks.

Overview of Admission Control for the Cisco CMTS

Admission Control on the Cisco CMTS is a mechanism that gracefully manages service flow 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. Admission Control monitors such resources constantly, and accepts or drops requests depending on the resource availability.

Admission Control 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. Admission Control reduces the impact of unpredictable traffic demands in circumstances that would otherwise produce degraded QoS for subscribers.

Admission Control 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, Admission Control verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

Admission Control 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. Admission Control checks are performed before the flow is committed.

Admission Control in Cisco IOS Release 12.3(13a)BCBC monitors the following resources on the Cisco CMTS.

- *CPU utilization*—Admission Control 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)*—Admission Control 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*—Admission Control monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

Note See also the "Admission Control and Cisco CMTS Resources" section on page 1-6.

Note Admission Control 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.

Admission Control 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 Admission Control with the following topics:

Admission Control and Cisco Universal Broadband Routers

Admission Control on the Cisco uBR10012 Universal Broadband Router

Cisco IOS Release 12.3(13a)BCBC supports Admission Control on the Cisco uBR10012 router and all broadband processing engines.

Admission Control on the Cisco uBR7246VXR Universal Broadband Router

Cisco IOS release 12.2(13)BC supports Admission Control on the Cisco uBR7246VXR router.

Admission Control and Memory Requirements for the Cisco CMTS

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(13a)BCBC, 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

Admission Control and Cisco CMTS Resources

Admission Control with Cisco IOS Release 12.3(13a)BCBC 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(13a)BCBC 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 Admission Control for the Cisco CMTS" section on page 1-12.

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 Admission Control Based on CPU Utilization" section on page 1-15.

Admission Control and Memory Utilization

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 Admission Control is supported for memory on the main CPU in Cisco IOS Release 12.3(13a)BCBC, and not for the broadband processing engine line card memory.

For additional information, refer to the "Configuring Admission Control Based on Memory Resources" section on page 1-16.

Admission Control and Upstream or Downstream Bandwidth Utilization

Admission control allows you to control the bandwidth usage for various DOCSIS traffic types.

Note Throughout this document, bandwidth refers to actual throughput on the upstream or downstream.

Whenever a new event occurs, whether a cable modem registration or dynamic service request (PacketCable voice call), Admission Control checks for the bandwidth availability based on configured thresholds. For new voice calls (or other dynamic services), if a threshold has been crossed, the new service request is gracefully declined.

For cable modem registration, if a service flow request is initiated with a Constant Bit Rate (CBR) bandwidth request, and if the bandwidth is not available, the request is processed, but an alarm is generated. Admission Control does not block cable modems from coming online, even if it exceeds the thresholds set for Admission Control.

Therefore, the only service request that Admission Control might decline (when thresholds have been crossed) is non-emergency 911 voice calls.

For additional information, refer to the "How to Configure Admission Control for the Cisco CMTS" section on page 1-12.

Thresholds for Upstream or Downstream Bandwidth

Admission Control monitors upstream or downstream bandwidth consumption with minor, major, and critical thresholds. Admission Control generates alarm traps when bandwidth consumption crosses minor and major thresholds. For additional information, refer to the "How to Configure Admission Control for the Cisco CMTS" section on page 1-12.

Exclusive and Non-Exclusive Bandwidth Thresholds

In addition to minor and major thresholds, Admission Control 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, Admission Control checks if there is any non-exclusive bandwidth available. Any new service request is permitted only if sufficient non-exclusive bandwidth is available.

Admission Control and Downstream Bandwidth

Admission Control for downstream bandwidth supports data traffic and PacketCable voice.

The traffic is classified as voice if the flow is associated with a PacketCable gate.

All the other service flows with non-zero minimum reservation rate are classified as data traffic. Any service flow with zero minimum reserve rate is classified as the Best Effort traffic. The BEt traffic can use any non-exclusive or un-configured bandwidth. No admission control check is performed when the best effort flows are created.

Admission Control and Upstream Bandwidth

Admission Control based on upstream bandwidth allows you to control the bandwidth utilization for various scheduling services, as defined in the DOCSIS specification. The Admission Control check occurs during cable modem registration or during a dynamic service event such as a voice call.

The DOCSIS specification defines scheduling services to bind QoS parameters with the service flows for the upstream channels. The following scheduling services or scheduling types are defined:

- Best Effort (BE)
- Non-real-time polling service (NRTPS)
- Real-time polling service (RTPS)
- Unsolicited grant service with activity detection (UGS-AD)
- Unsolicited grant service (UGS)

Note Best Effort (BE) traffic in this case is the BE traffic with non-zero min-reservation rate. In the DOCSIS terminology this is referred to as Committed Information Rate (CIR) traffic. The BE traffic with zero min-reservation rate is referred to as "un-classified BE" traffic in this document. This unclassified BE traffic may use any exclusive or unused bandwidth.

For each upstream scheduling type, you can specify the following:

- The percentage of combined throughput that must be set aside [exclusive] for all the sessions of a particular scheduling type.
- The percentage of combined throughput that can be allocated [non-exclusive] for all the sessions of a particular scheduling type.

A service flow may be defined as a service-class template; with a service class name associated with it. This is typically defined in the DOCSIS configuration file. You can also set Admission Control thresholds for a specific service class. The thresholds for a service class are enveloped by the thresholds for the scheduling type it belongs to. In other words, the sum of exclusive thresholds for all the service classes of a particular scheduling type should be less than the exclusive threshold for that scheduling type.

Note Upstream DOCSIS service classes must be defined on the Cisco CMTS prior to the configuration of Admission Control.

For additional information, refer to the "Configuring Admission Control Based on Upstream Bandwidth" section on page 1-22.

Precedence of the Configuration Commands

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

If you configure both interface-level and global thresholds for Admission Control, and then you remove interface-level configurations, the global configuration thresholds become effective for that interface.

When globally configured, all the interfaces (either DS or US) assume the same global configuration. If bandwidth is configured for an interface, in addition to or instead of global configuration, the thresholds set for an interface override the global threshold values. Also, for upstream bandwidth, if an individual upstream is configured, it overrides the interface-level or the global configuration values.

Note Thresholds applied to the US or DS bandwidth apply to the physical interfaces. Admission Control configuration commands are not applicable to virtual interfaces such as sub-interfaces or bundling interfaces.

Admission Control and Additional Features on the Cisco CMTS

Admission Control and High Availability Features

In Cisco IOS Release 12.3(13a)BCBC, Admission Control configurations interact with high availability features in the following ways for HCCP N+1 Redundancy and Route Processor switchover events.

Admission Control with HCCP N+1 Redundancy on the Cisco CMTS

When HCCP N+1 Redundancy is configured on the Cisco uBR10012 router, Admission Control configurations are maintained during planned or unplanned switchover events between HCCP Working and Protect interfaces. Traffic and services experiencing such switchover events automatically maintain Admission Control resource allocation, including prioritization of Emergency 911 voice calls.

For configuration information, refer to *N+1 Redundancy for the Cisco Cable Modem Termination System*.

Admission Control with Route Processor Redundancy Plus on the Cisco uBR10012 Router

When RPR+ redundancy is configured on the Cisco uBR10012 router, the configured parameters are conserved during PRE module switchover from the Primary RP to the Secondary RP. The command line interface configurations are synchronized between the two and supported during switchover, but note the following counters and statistics:

- Admission Control counters and statistics for CPU and memory resources are lost during a PRE switchover event.
- Admission Control bandwidth resources (DS and US counters and statistics) are maintained at the line card and retained.

For general RPR+ configuration information, refer to *Route Processor Redundancy Plus on the Cisco uBR10012 Universal Broadband Router* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/u10krprp.html

Admission Control and Load Balancing

Load Balancing on the Cisco CMTS provides efficient upstream and downstream bandwidth utilization. Load balancing provides these advantages, for interaction with Admission Control:

- Static support—balances upstream and downstream channels when the Cable Modems registers.
- Dynamic support—monitors and balances the channel load in real-time during operation.

The cable modems that move across upstream or downstream as a part of Dynamic Load Balancing may have an active voice call at any one time. Therefore, the UCC (Upstream Channel Change) and DCC (Downstream Channel Change) verify that resources are not violated with Admission Control in the following ways:

- For CPU utilization, because the main CPU processor resource is only being considered, when the cable modem moves to a different upstream or downstream, the effective CPU at the CMTS is not affected and therefore, there is no Admission Control check performed at the CPU, even when Admission Control is configured for CPU utilization.
- For memory, as with CPU utilization, only the main CPU memory resource is being regulated. Therefore, when a cable modem moves, there are negligible effects, and no Admission Control check is needed.
- For upstream DOCSIS bandwidth, when a cable modem moves to a new upstream channel, the Admission Control criteria for the new channel should not be violated. Therefore, during the load balancing event, the Admission Control check is performed. If the threshold requirements for the new channel are not met, the channel transition is blocked.

  For example, consider a case where an upstream channel Upstream1 with 70% of the total load moves a cable modem with a UGS flow to another channel Upstream2 with only 20% load. If the Upstream2 is configured for only 18% of admission control threshold for the UGS flows, the transition will fail.
- For downstream DOCSIS bandwidth, similar to the upstream scenario, load balancing a cable modem to a new downstream channel with insufficient bandwidth available could interrupt the attempted load balancing.

For additional information about load balancing on the Cisco CMTS, refer to the following document on Cisco.com:

- *Load Balancing for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmtslbg.html

Admission Control and Spectrum Management

Admission Control in Cisco IOS Release 12.3(13a)BCBC also works in conjunction with spectrum management and frequency hopping, when they are configured on the Cisco router. Such bandwidth is allocated as a percentage, and this percentage and associated thresholds are maintained across frequency hopping. Admission Control generates an alarm if voice calls are dropped while the bandwidth utilization is still lower than the combined exclusive and non-exclusive bandwidth.

Admission Control provides limited support for spectrum management and frequency hopping. With these features, all traffic on one channel may be moved to another frequency, and the new channel may have lower effective data rate than the original channel. The Admission Control threshold limits are preserved during this transition, however this may result in inconsistent bandwidth allocation for different traffic types. Therefore, Cisco recommends that during frequency hopping, the new channel have the same effective data rate as the original channel when Admission Control is enabled.

How to Configure Admission Control for the Cisco CMTS

Admission Control is not configured by default on the Cisco router. It is necessary to configure and to enable Admission Control according to the specific resources and traffic types to be supported. This section describes the following configuration procedures for Admission Control on the Cisco CMTS, in the recommended sequence in which they should be configured. Not all resource types have to be configured for Admission Control operation, but Admission Control Event Types must be configured first.

- Enabling Admission Control for Event Types, page 1-13

  This procedure sets the events that trigger the Admission Control checks on the Cisco CMTS.

- Configuring Admission Control Based on CPU Utilization, page 1-15

  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 Admission Control Based on Memory Resources, page 1-16

  This procedure configures memory resource types and associated threshold levels for Admission Control on the Cisco CMTS.

- Validity Checks for Bandwidth Admission Control, page 1-18

  To prevent circumstances in which some Admission Control configurations are inconsistent, Admission Control first validates the attempted configuration, and if an error is found, Admission Control prints an error message and the configuration is not set.

- Configuring Admission Control Based on Downstream Bandwidth, page 1-18

  This procedure configures exclusive or non-exclusive downstream bandwidth allocation, whether in in global or interface level. This procedure also configures minor and major thresholds for optimized downstream QoS support.

- Configuring Admission Control Based on Upstream Bandwidth, page 1-22

  This procedure configures exclusive or non-exclusive upstream bandwidth allocation. This configuration can be implemented in global, interface, or per-upstream levels. This procedure also configures minor and major thresholds that monitor and maintain optimized DOCSIS QoS for upstream traffic.

- Calculating Upstream and Downstream Bandwidth Utilization, page 1-32

  Provides guidelines for calculating actual upstream or downstream bandwidth consumption.

Enabling Admission Control for Event Types

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

- the registration of a cable modem
- the request for a voice call, whether a PacketCable voice call or other dynamic service

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

Prerequisites

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 Admission Control for the Cisco CMTS" section on page 1-2.

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 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 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 but calls from the cable modem would be rejected.
		• **dynamic-service**—Sets Admission Control checks to be performed when 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 Admission Control traffic event activity on the Cisco CMTS can be reviewed using the following two commands:

- **debug cable admission-control**
- **RTPS - 14 0 18 0 25 0 5**

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

Configuring Admission Control Based on CPU Utilization

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.

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. 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. 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 Admission Control for the Cisco CMTS" section on page 1-2.

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 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 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 Admission Control is supported for memory on the main CPU in Cisco IOS Release 12.3(13a)BCBC, 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 Admission Control for the Cisco CMTS" section on page 1-2.

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# need two new examples`
		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-configure.

Validity Checks for Bandwidth Admission Control

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 Admission Control configurations are inconsistent, Admission Control first validates the attempted configuration, and if an error is found, 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, 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 scheduling types. If exclusive thresholds for UGS, UGS-AD, RTPS, and nRTPS traffic were configured at 15% each, this would mean a total of 60% bandwidth is exclusively reserved for these US scheduling types. This leaves only 40% for any non-exclusive bandwidth. Therefore, in this case, the maximum non-exclusive thresholds that any scheduling type can have is 40% (100% - 60%), and should be less than 40%.
3. For upstream bandwidth, the total exclusive thresholds for all service classes (for a given scheduling type) should be less than the exclusive threshold for that scheduling type. For example, consider a circumstance with UGS service classes ugs_class1 and ugs_class2 scheduling types are configured. If the exclusive threshold for scheduling type UGS is set at 50%, then the sum of thresholds for ugs_class1 and ugs_class2 should not exceed 50%. Therefore, the exclusive bandwidth for the scheduling type includes the exclusive bandwidth allocation for the service classes of that scheduling type.
4. For upstream bandwidth, the non-exclusive bandwidth for a given scheduling type should be greater than the maximum non-exclusive value for all the service classes configured within that scheduling type. Therefore, if you configure the non-exclusive threshold for the UGS scheduling type as 20%, then the non-exclusive threshold for the service classes ugs_class1 or ugs_class2 cannot exceed 20%.

Caution Admission Control validates bandwidth threshold with validation checks, but only for the traffic types that are configured. Otherwise, Admission Control does not validate resource configurations. For example if you configure DS bandwidth Admission Control for CIR data at 40% exclusive threshold. You are implicitly limiting the voice usage to 60% of the bandwidth. However if you don't set any threshold for voice, the voice Admission Control check will not be performed. Thus, the new calls will be accepted without any Admission Control checks. Potentially the voice usage may exceed the implicit limit of 60% bandwidth, and occupy the 40% bandwidth reserved exclusively for the data. To avoid this problem, configure Admission Control for all the traffic types in a given direction (US or DS). In the example above, voice thresholds are configured so that the sum of exclusive and non-exclusive thresholds is less than 60% of the total resource available.

For additional information, refer to the "Configuring Admission Control Based on Downstream Bandwidth" section on page 1-18.

Configuring Admission Control Based on Downstream Bandwidth

Admission Control based on downstream bandwidth allows you to control the bandwidth utilization for voice or data traffic. The Admission Control check is made during cable modem registration or during a dynamic service event such as a voice call.

Note There are no scheduling types that exist for downstream as they do for upstream.

Admission Control makes decisions based on the total downstream DOCSIS throughput that is used when compared against the total downstream DOCSIS throughput that is available.

Downstream thresholds can be configured in either of these two ways:

- All downstream cable interfaces s on the Cisco router can configured for Admission Control at one time in global configuration mode.
- All downstream ports on each selected cable interface can be configured for Admission Control in interface configuration mode.

Perform the following steps to configure and enable downstream threshold levels on the Cisco CMTS.

Prerequisites

Refer to the "Prerequisites for Admission Control for the Cisco CMTS" section on page 1-2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. (Optional) **interface cable** {*slot* | *subslot*} {*slot*/*subslot*/*port*}
4. **[no] cable admission-control ds-bandwidth** <*traffic-type*> **minor** <*minor-threshold*> **major** <*major-threshold*> **exclusive** <*exclusive-percentage*> [**non-exclusive** <*non-exclusive-percentage*>]
5. **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	**interface cable** {*slot* | *subslot*} {*slot*/*subslot*/*port*} **Example:** `Router(config)# interface c8/0/1`	(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.

	Command or Action	Purpose
Step 4	**[no] cable admission-control ds-bandwidth** <*traffic-type*> **minor** <*minor-threshold*> **major** <*major-threshold*> **exclusive** <*exclusive-percentage*> [**non-exclusive** <*non-exclusive-percentage*>] **Example:** `Router(config)# cable admission-control ds-bandwidth voice minor 15 major 25 exclusive 30 non-exclusive 15`	Global configuration sets minor, major and exclusive thresholds for downstream voice or data bandwidth for all interfaces on the Cisco CMTS. Repeat this step when setting bandwidth for both voice and data. 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. • *traffic-type*—Either of the following keywords sets the traffic type for which Admission Control applies. Both settings can be applied to the Cisco CMTS. – **voice**—Applies thresholds to downstream voice traffic. – **data**—Applies thresholds to downstream data traffic. • **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 class 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 classes as specified. The **no** form of this command removes downstream bandwidth from the Cisco CMTS: • **no cable admission-control ds-bandwidth**
Step 5	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

Example of Admission Control for Downstream Traffic

This example illustrates a sample configuration for 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 voice minor 15 major 25 exclusive 30
```

In this example, the voice calls are rejected when the bandwidth usage of the voice calls exceeds 30%In addition, you can allow for some flexibility by allowing voice 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 voice minor 15 major 25 exclusive 30
non-exclusive 20
```

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

Similarly you can configure data thresholds as follows:

```
Router(config)# cable admission control downstream data 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 1-6 summarizes this throughput distribution:

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

Throughput Type	% Configured	% Consumed	% Available
Voice	30%	20%	10%
Data	50%	40%	10%
Best Effort (unclassified)		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.
- Best Effort gives up 10% of available non-exclusive throughput to voice traffic.

Table 1-3 summarizes this throughput distribution:

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

Throughput Type	% Configured	% Consumed	% Available
Voice	30%	40% (30% + 10%)	0%
Data	50%	50%	0%
Best Effort (unclassified)		0%	10% (100% - 40% - 50%)

Step 3—Data Throughput 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 1-4 summarizes this throughput distribution:

Table 1-4 Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	% Configured	% Consumed	% Available
Voice	30%	40% (30% + 10%)	0%
Data	50%	60% (50% + 10%)	0%
Best Effort (unclassified)			0% (100%-40%-60%)

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

Stage 4—Voice Throughput Consumption Increases by another 10%

Now assume that additional voice calls arrive and voice requires all 20% of non-exclusive (Best Effort) throughput on the Cisco CMTS. Because voice can preempt data traffic, voice displaces the 10% of non-exclusive throughput being used by data, and voice now consumes all non-exclusive throughput for a new total of 50%. Data throughput consumption is reduced from 60% back to 50%.

Table 1-5 summarizes this throughput distribution:

Table 1-5 Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	% Configured	% Consumed	% Available
Voice	30%	50% (30% + 20%)	0%
Data	50%	50%	0%
Best Effort (unclassified)	20%	0%	0%

Note that more voice calls not be admitted because voice has used up its exclusive and non-exclusive share of throughput on the Cisco CMTS.

Configuring Admission Control Based on Upstream Bandwidth

Admission Control based on upstream bandwidth allows you to control the bandwidth utilization for various scheduling services defined in DOCSIS. Admission Control performs checks during cable modem registration or during a dynamic service event such as a voice call.

DOCSIS defines Service flow scheduling services to bind QOS parameters with the service flows for the upstream channels. The following scheduling services or scheduling types are defined:

- Best Effort (BE)
- Non-real-time polling service (NRTPS)
- Real-time polling service (RTPS)
- Unsolicited grant service with activity detection (UGS-AD)
- Unsolicited grant service (UGS)

Some service flows may also have service-class names associated with them.

- The percentage of combined throughput that must be set aside [exclusive] for all the sessions of a particular scheduling type

- The percentage of combined throughput that can be allocated [non-exclusive] for all the sessions of a particular scheduling type

A service flow may be defined as a service-class template; with a service class name associated with it. This is typically defined in the DOCSIS confide file. You can also set Admission Control thresholds for a specific service class. The thresholds for a service class are enveloped by the thresholds for the scheduling type to which it belongs.

In other words, the sum of exclusive thresholds for all the service classes of a particular scheduling type should be less than the exclusive threshold for that scheduling type. The upstream thresholds can be configured at the following three levels:

- Global configuration mode—applies threshold settings to the CMTS in global fashion (all interfaces and all upstreams).
- Interface configuration mode for interface configuration—applies thresholds only to the specified interface. This value supersedes the global settings when both of them are configured.
- Interface configuration mode for per-upstream configuration—applies thresholds only to the specified upstream. This value supersedes the value in either of the above settings when per-upstream is configured in combination with them.

Note Upstream DOCSIS service classes must be defined on the Cisco CMTS prior to the configuration of Admission Control for those service classes.

Perform the following steps to configure and enable upstream throughput threshold levels on the Cisco CMTS.

Prerequisites

Refer to the "Prerequisites for Admission Control for the Cisco CMTS" section on page 1-2.

SUMMARY STEPS

Global Configuration

1. **enable**
2. **configure terminal**
3. **cable admission-control us-bandwidth** [**sched** <*sched-type*> | **service** <*service-class-name*>] **minor** <*minor-threshold*> **major** <*major-threshold*> **exclusive** <*exclusive-percentage*> [**non-exclusive** <*non-exclusive-percentage*>]
4. **Ctrl-Z**

Interface Configuration

1. **enable**
2. **configure terminal**
3. **interface cable** [*slot/port* | *slot/sublot/port*]
4. **cable upstream** <*n*> **admission-control us-bandwidth** [**sched** <*sched-type*> | **service** <*service-class-name*>] **minor** <*minor-threshold*> **major** <*major-threshold*> **exclusive** <*exclusive-percentage*> [**non-exclusive** <*non-exclusive-percentage*>]
5. **Ctrl-Z**

Upstream Port Configuration

1. **enable**
2. **configure terminal**
3. **interface cable** [*slot/port* | *slot/sublot/port*]
4. **cable upstream** <*port-no*> **admission-control us-bandwidth** [**sched** <*sched-type*> | **service** <*service-class-name*>] **minor** <*minor-threshold*> **major** <*major-threshold*> **exclusive** <*exclusive-percentage*> [**non-exclusive** <*non-exclusive-percentage*>]
5. **Ctrl-Z**

DETAILED STEPS FOR GLOBAL CONFIGURATION

	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	**cable admission-control us-bandwidth** [**sched** *<sched-type>* | **service** *<service-class-name>*] **minor** *<minor-threshold>* **major** *<major-threshold>* **exclusive** *<exclusive-percentage>* [**non-exclusive** *<non-exclusive-percentage>*] **Example:** `Router(config)# cable admission-control us-bandwidth scheduling-type RTPS minor 10 major 20 exclusive 30 non-exclusive 10`	Configures global upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS. • **us-bandwidth**—Specifies that this command is to configure the upstream bandwidth thresholds. • **sched** <*sched-type*>—Specifies the scheduling type for a traffic class; <*sched-type*> can have the following possible values: – **BE—**selects best effort traffic – **NRTPS—**selects non-real-time polling service – **RTPS**—selects real time polling service – **UGS-AD—**for UGS-AD service – **UGS**—for UGS service • **service** <*service-class-name*>—Alphanumeric string representing a previously defined service class name. Instead of specifying a class by a scheduling type, the service class name can be used as a keyword to select the service class. **Note** Refer to cable service class command in the *Cisco Broadband Cable Command Reference Guide*. • **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 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

DETAILED STEPS FOR INTERFACE CONFIGURATION

	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	**interface cable** [*slot/port* | *slot/sublot/port*] **Example:** `Router(config)# interface c8/0/1`	Enters interface configuration mode for the specified port. The Cisco universal broadband routers differ in slot selection as follows: • *slot/subslot/port*—For the Cisco uBR10012 router, *slot* can range from 5 to 8, *subslot* can be 0 or 1, and *port* can be 0 to 4 (depending on the cable interface) • *slot/port*—On the Cisco uBR7246VXR router, *slot* can range from 3 to 6, and *port* can be 0 or 1, depending on the cable interface.
Step 4	**cable admission-control us-bandwidth** [**sched** <*sched-type*> | **service** <*service-class-name*>] **minor** <*minor-threshold*> **major** <*major-threshold*> **exclusive** <*exclusive-percentage*> [**non-exclusive** <*non-exclusive-percentage*>] **Example:** `Router(config-if)# cable admission-control us-bandwidth sched UGS minor 30 major 35 exclusive 40 non-exclusive 10`	Enables Admission Control for upstream throughput on the specified interface and all associated upstreams. • **us-bandwidth**—Specifies that this command is to configure the upstream throughput thresholds. • **sched** <*sched-type*>—Specifies the scheduling type for a traffic class; <*sched-type*> can have the following possible values: – **BE—**selects best effort traffic – **NRTPS—**selects non-real-time polling service – **RTPS**—selects real time polling service – **UGS-AD—**for UGS-AD service – **UGS—**for UGS service • **service** <*service-class-name*>—A string representing a previously defined service class. Instead of specifying a class by a scheduling type, this keyword can be used to specify a class using the *service-class-name*. • **minor** <*minor-threshold*>—Sets the minor alarm threshold. • **major** <*major-threshold*>—Sets the major alarm threshold. • **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 an integer between 1 and 100. No other class 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 classes as specified.

Step 5	**Ctrl-z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

DETAILED STEPS FOR PORT-LEVEL CONFIGURATION

	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	**interface cable** [*slot/port* | *slot/sublot/port*] **Example:** `Router(config)# interface c8/0/1`	Enters interface configuration mode for the specified port. The Cisco universal broadband routers differ in slot selection as follows: • *slot/subslot/port*—For the Cisco uBR10012 router, *slot* can range from 5 to 8, *subslot* can be 0 or 1, and *port* can be 0 to 4 (depending on the cable interface) • *slot/port*—On the Cisco uBR7246VXR router, *slot* can range from 3 to 6, and *port* can be 0 or 1, depending on the cable interface.

Step 4	**cable upstream** <*n*> **admission-control us-bandwidth** [**sched** <*sched-type*> | **service** <*service-class-name*>] **minor** <*minor-threshold*> **major** <*major-threshold*> **exclusive** <*exclusive-percentage*> [**non-exclusive** <*non-exclusive-percentage*>] **Example:** `Router(config-if)# cable upstream admission-control us-bandwidth sched UGS minor 30 major 35 exclusive 40 non-exclusive 10`	Enables Admission Control for upstream throughput on the specified port. This configuration must be present on every upstream port in the Cisco CMTS for optimal upstream granularity. • **upstream**—Applies the configuration to the specified upstream, overriding previous threshold configurations that may exist on the interface or Cisco CMTS. • *n—slot/port* on the Cisco uBR7246VXR router, *slot/subslot/port* on the Cisco uBR10012 router. • **us-bandwidth**—Specifies that this command is to configure the upstream throughput thresholds. • **sched** <*sched-type*>—Specifies the scheduling type for a traffic class; <*sched-type*> can have the following possible values: – **BE—**selects best effort traffic – **NRTPS—**selects non-real-time polling service – **RTPS**—selects real time polling service – **UGS-AD—**for UGS-AD service – **UGS—**for UGS service • **service** <*service-class-name*>—A string representing a previously defined service class. Instead of specifying a class by a scheduling type, this keyword can be used to specify a class using the *service-class-name*. • **minor** <*minor-threshold*>—Sets the minor alarm threshold. • **major** <*major-threshold*>—Sets the major alarm threshold. • **exclusive** <*exclusive-percentage*>—Sets the critical threshold for the upstream bandwidth resource. <*exclusive-percentage*> is an integer between 1 and 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. <non-exclusive-percentage> is an integer between 1 and 100. Since this bandwidth is non-exclusive, it can be used by other classes as specified (see examples below). Note that non-exclusive share for BE traffic is 100% by default. If other sessions of other classes come in, they will be admitted by preempting the non-exclusive share of BE traffic.
Step 5	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

Example of Admission Control with Upstream Traffic Types

This example illustrates a sample configuration in which upstream bandwidth (throughput) as follows:

- 40% reserved exclusively for UGS traffic.
- 15% reserved exclusively for RTPS traffic.
- Minor and major alarms for UGS generated at 30% and 35% respectively.
- Minor and major alarms for RTPS traffic generated at 8% and 12% respectively.

The following two Cisco IOS commands implement this configuration for UGS and RTPS.

```
Router(config)# cable admission-control us-bandwidth scheduling type UGS minor 30 major 35
exclusive 40
Router(config)# cable admission-control us-bandwidth scheduling type RTPS minor 8 major 12
exclusive 15
```

This initial configuration accomplishes the following Quality of Service policy on the Cisco CMTS:

- If the UGS traffic exceeds 40%, additional UGS flows are denied.
- Similarly if the RTPS traffic exceeds 15%, additional RTPS flows are denied.
- Unclassified Best Effort traffic in this case has access to the remaining throughput of 45% (subtracting 55% from 100%), and non-exclusive access to 100% of the total throughput.

Further flexibility in the Quality of Service policy in this scenario can be accomplished as follows. In addition to the above percentages reserved exclusively for the UGS and RTPS classes, you can allow for UGS flows to exceed their exclusive share, and to consume up to 50% of the upstream throughput.

The following two Cisco IOS commands implement this additional configuration. Commands apply to UGS and RTPS respectively:

```
Router(config)# cable admission-control us-bandwidth scheduling type UGS minor 30 major 35
exclusive 40 non-exclusive 10
Router(config)# cable admission-control us-bandwidth scheduling type RTPS minor 8 major 12
exclusive 15
```

The following multi-stage scenario illustrates how the lending and borrowing of throughput is achieved in the presence of multiple traffic classes and their varying percentages over time.

Stage I—Initial Throughput Allocations

As defined by the above commands, the throughput is initially allocated as follows, assuming the following traffic:

- UGS flows are allocated 40% exclusive throughput, and current usage is 30%.
- RTPS flows are allocated 15% exclusive throughput and current usage is 15%.
- Unclassified Best Effort traffic in this case has access to the remaining throughput of 45% (subtracting 55% from 100%). The unclassified BE traffic may also use the 55% of the exclusive bandwidth if it is not in use. The unclassified BE traffic may use 45% remaining bandwidth, but uses 30%.

Table 1-6 summarizes this throughput distribution:

Table 1-6 Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	% Configured	% Consumed	% Available
UGS	40%	30%	10%
RTPS	15%	15%	0%
Best Effort		30%	15%

Stage 2—UGS Requires Additional Throughput

Now assume that UGS throughput consumption increases to 45% total. This is 5% over its exclusive allocation. In response to this change in traffic requirements, UGS takes an additional 5% throughput from its non-exclusive pool. Total throughput available for unclassified Best Effort is now reduced to 40%.

The following conditions otherwise remain unchanged:

- RTPS throughput consumption remains at 15%.
- Unclassified Best Effort throughput consumption remains at 30%.

Table 1-7 summarizes this change in throughput allocation, consumption and availability

Table 1-7 Throughput Allocation and Consumption for Stage 2 of this Example

Throughput Type	% Configured	% Consumed	% Available
UGS	40%	45% (40% + 5%)	0%
RTPS	15%	15%	0%
Best Effort		30%	10%

Stage 3—Best Effort Traffic Attempts to Exceed (Non-exclusive) Throughput

Now assume that Best Effort data traffic increases to consume all 40% of non-exclusive throughput, then attempts to exceed this threshold. In response, the Cisco CMTS gracefully declines additional call requests in Best Effort traffic (beyond 40% consumption).

The following conditions otherwise remain unchanged:

- UGS throughput consumption remains at 45% (no additional throughput available).
- RTPS throughput consumption remains at 15% (with no additional throughput remaining).

Table 1-8 summarizes this change in throughput allocation, consumption and availability

Table 1-8 Throughput Allocation and Consumption for Stage 3 of this Example

Throughput Type	% Configured	% Consumed	% Available
UGS	40%	45% (40% + 5%)	0%
RTPS	15%	15%	0%
Best Effort		40%	0%

Stage 4—UGS Requires Additional Throughput

Now assume that UGS requires an additional 5% throughput. UGS now consumes 50% total throughput. In response to this change, UGS claims and displaces 5% throughput from Best Effort's active throughput. In response to that, Best Effort traffic is reduced to 35%, without disruption to RTPS consumed bandwidth.

Note For the first time in this multi-stage example, throughput consumption on the Cisco CMTS has reached 100%, and there is no additional throughput available on the Cisco CMTS after the events of Stage 4.

The following conditions otherwise remain unchanged in Stage 4:

- The RTPS throughput consumption remains at 15%, but with no additional throughput available.

Table 1-9 summarizes this change in throughput allocation, consumption and availability

Table 1-9 Throughput Allocation and Consumption for Stage 4 of this Example

Throughput Type	% Configured	% Consumed	% Available
UGS	40%	50% (40% + 5% + 5%)	0%

Table 1-9 Throughput Allocation and Consumption for Stage 4 of this Example

Throughput Type	% Configured	% Consumed	% Available
RTPS	15%	15%	0%
Best Effort		35%	0%

What to Do Next

Once configured, upstream traffic activity and events on the Cisco CMTS can be reviewed using the following two commands:

- **debug cable admission-control**
- **RTPS - 14 0 18 0 25 0 5**

Calculating Upstream and Downstream Bandwidth Utilization

The 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, 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, 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. 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, 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 factor 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 Admission Control threshold that is set, and no calls may be scheduled after 85 calls.

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

How to Troubleshoot Admission Control for the Cisco CMTS

Admission Control supports multiple resources within a Quality of Service policy. The first step in monitoring and troubleshooting Admission Control is to enable automatic debugging for any of the following resources, as required:

- Debugging Admission Control for Different Event Types, page 1-33
- Debugging Admission Control for CPU Resources, page 1-33
- Debugging Admission Control for Memory Resources, page 1-34
- Debugging Admission Control for Downstream Bandwidth, page 1-34
- Debugging Admission Control for Upstream Throughput, page 1-34

Debugging Admission Control for Different Event Types

To enable event-oriented troubleshooting for Admission Control, use the **debug cable admission-control event** command in privileged EXEC mode.

```
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
```

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

- **debug cable admission-control**
- **RTPS - 14 0 18 0 25 0 5**
- "How to Configure Admission Control for the Cisco CMTS" section on page 1-12

Debugging Admission Control for CPU Resources

To enable CPU troubleshooting processes for Admission Control, use the **debug cable admission-control cpu** command in privileged EXEC mode.

```
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
```

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

- **debug cable admission-control**
- **RTPS - 14 0 18 0 25 0 5**
- "How to Configure Admission Control for the Cisco CMTS" section on page 1-12

Debugging Admission Control for Memory Resources

To enable memory troubleshooting processes for Admission Control, use the **debug cable admission-control memory** command in privileged EXEC mode.

```
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
```

If 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**
- **RTPS - 14 0 18 0 25 0 5**
- "How to Configure Admission Control for the Cisco CMTS" section on page 1-12

Debugging Admission Control for Downstream Bandwidth

To enable downstream throughput troubleshooting processes for Admission Control, use the **debug cable admission-control ds-bandwidth** command in privileged EXEC mode.

```
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
```

If Admission Control checks fail for the downstream, refer to the following sections for additional information about throughput thresholds, events and configuration:

- **debug cable admission-control**
- **RTPS - 14 0 18 0 25 0 5**
- "How to Configure Admission Control for the Cisco CMTS" section on page 1-12

Debugging Admission Control for Upstream Throughput

To enable upstream throughput troubleshooting processes for Admission Control, use the **debug cable admission-control us-bandwidth** command in privileged EXEC mode.

```
Router# debug cable admission-control us-bandwidth
```

```
R7612-ubr10k#
Oct 8 23:29:11: Failed to allocate US bandwidth for
CM 0007.0e01.9b45 in adding a new service entry
```

If Admission Control checks fail for the upstream, refer to the following sections for additional information about throughput thresholds, events and configuration:

- **debug cable admission-control**
- **RTPS - 14 0 18 0 25 0 5**
- "How to Configure Admission Control for the Cisco CMTS" section on page 1-12

Configuration Examples of Admission Control for the Cisco CMTS

There may be situations where multiple resources on the Cisco CMTS compete for the same throughput. In these cases, Admission Control implements the following levels of priority:

- Best Effort (BE) service has the lowest priority for throughput.
- Services with exclusive rights have precedent over Best Effort service, but they have the same priority in relation to each other.

Therefore, if BE traffic is competing with other traffic for throughput, the other service classes get priority. When two or more non-BE service classes compete for the same throughput, they share throughput on a first come first serve basis. This is illustrated in the examples that follow.

This section provides or links to examples of Admission Control in which throughput is either shared across multiple resources in non-exclusive fashion, or allocated exclusively and not shared:

- Example of Admission Control for Downstream Traffic, page 1-20
- Example of Admission Control with Upstream Traffic Types, page 1-29
- Example of Admission Control in Non-shared Configuration, page 1-35
- Example of Admission Control in Shared Configuration with Best Effort Traffic, page 1-36
- Example of Admission Control in Shared Configuration without Best Effort Traffic, page 1-36

Example of Admission Control in Non-shared Configuration

This is an example of Admission Control in which UGS and RTPS retain exclusive and non-exclusive shares of throughput, as follows:

- UGS—exclusive share is 40%, non-exclusive share is 10%.
- RTPS—exclusive share is 40%, non-exclusive share is 10%.

In this example, the exclusive shares add up to 80%. Therefore, 20% of the throughput on the Cisco CMTS is available to both of the classes. Because the non-exclusive share is configured as 10% to each, the sessions of each class do not compete with each other. Requests for both UGS and RTPS can be satisfied simultaneously, and there is no need to share any throughput on the Cisco CMTS.

Example of Admission Control in Shared Configuration with Best Effort Traffic

This is an example of Admission Control in which UGS and RTPS share resources with each other and with Best Effort traffic, as follows:

- UGS—exclusive share is 40%, non-exclusive share is 20%.
- RTPS—exclusive share is 20%, non-exclusive share is 20%.
- BE—exclusive share is 20%.

In this example, the exclusive throughput allocation totals 80%, and 20% of the throughput is left as non-exclusive throughput, which is shared. Because UGS and RTPS are each configured with a non-exclusive percentage of 20%, this 20% of the throughput is shared between UGS and RTPS. In addition to these classes, the BE class can also share this throughput. However, because the BE class has non-exclusive bandwidth only, it can be preempted by either UGS or RTPS classes when they compete for the same 20% of bandwidth on a first-come, first-served basis.

Example of Admission Control in Shared Configuration without Best Effort Traffic

This is an example of Admission Control in which UGS and RTPS share resources with non-exclusive Best Effort throughput, with no Best Effort traffic or throughput consumption:

- UGS—exclusive share is 40%, non-exclusive share is 10%.
- RTPS—exclusive share is 50%, non-exclusive share is 10%.

In this example, the exclusive throughput for all classes totals 90%, and 10% of the throughput on the Cisco CMTS is left as non-exclusive throughput. Because non-exclusive share for both classes is configured as 10% each, and because UGS and RTPS have equal priority, they share this 10% on a first-come, first-served basis.

```
RTPS      -     14     0      18      0      25         0       5
BE        -     16     21     18      20     20         100     5

Resource - Downstream Bandwidth
Flow   Minor  # of   Major   # of   Excls  # of   Non-Excls  Curr.  Conf
Type   Level  Times  Level   Times  Level  Times  Level      Reserv Level
voice  35     10     40      8      45     6      0          38     I
```

Admission Control MIB Specifications for the Cisco CMTS

Cisco IOS Release 12.3(13a)BCBC introduces new SNMP MIBs and objects for Admission Control. The primary MIBs for Admission Control on the Cisco CMTS are supported in three types:

- configuration attributes
- monitoring attributes
- SNMP notifications

This section provides the following MIB information for Admission Control in Cisco IOS Release 12.3(13a)BCBC:

General MIB Information for Admission Control

MIBs for Admission Control on the Cisco CMTS

MIB Objects for Admission Control Configuration

MIB Objects for Admission Control Monitoring

For additional MIB information for the Cisco CMTS, refer to these resources on Cisco.com:

- *Cisco CMTS MIB Specifications Guide*:

  http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html
- Cisco MIB Web page:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Compliance, Conformance, and Capability Information for Admission Control

Compliance Statements for Admission Control

Admission Control in Cisco IOS Release 12.3(13a)BC uses the following compliance-related objects:

- **ciscoCableAdmCtrlCompliances** object identifier

  ::= { ciscoCableAdmCtrlMIBConform 1 }

- **ciscoCableAdmCtrlMIBGroups** object identifier

  ::= { ciscoCableAdmCtrlMIBConform 2 }

- **ciscoCableAdmCtrlCompliance** module (::= {ciscoCableAdmCtrlCompliances 1}) —This compliance statement contains entities that implement the Cisco Cable Admission Control MIB. Mandatory groups within this module are as follows:
  - ciscoCableAdmCtrlConfigGroup
  - ciscoCableAdmCtrlStatGroup
  - ciscoCableAdmCtrlEventHistGroup
  - ciscoCableAdmCtrlNotifGroup

  The ciscoCableAdmCtrlCompliance module contains the following objects. Each of these have MIN-ACCESS setting of read-only. Write and create access are not required.
  - ccacSysRscConfigStatus
  - ccacSysRscConfigMinorThreshold
  - ccacSysRscConfigMajorThreshold
  - ccacSysRscConfigCritThreshold
  - ccacUsConfigStatus
  - ccacUsConfigMinorThreshold
  - ccacUsConfigMajorThreshold
  - ccacUsConfigExclusivePercent
  - ccacUsConfigNonExclusivePercent
  - ccacDsConfigStatus
  - ccacDsConfigMinorThreshold
  - ccacDsConfigMajorThreshold
  - ccacDsConfigExclusivePercent
  - ccacDsConfigNonExclusivePercent

MIB Units of Conformance for Admission Control

The following object groups and associated objects for Admission Control pertain to MIB units of conformance:

- **ciscoCableAdmCtrlConfigGroup** (::= {ciscoCableAdmCtrlMIBGroups 1}) —This collection of objects provides the event monitoring and notification configuration:
  - ccacNotifyEnable,
  - ccacEventMonitoring,

  - ccacSysRscConfigStatus,
  - ccacSysRscConfigMinorThreshold,
  - ccacSysRscConfigMajorThreshold,
  - ccacSysRscConfigCritThreshold,
  - ccacUsConfigStatus,
  - ccacUsConfigMinorThreshold,
  - ccacUsConfigMajorThreshold,
  - ccacUsConfigExclusivePercent,
  - ccacUsConfigNonExclusivePercent,
  - ccacDsConfigStatus,
  - ccacDsConfigMinorThreshold,
  - ccacDsConfigMajorThreshold,
  - ccacDsConfigExclusivePercent,
  - ccacDsConfigNonExclusivePercent
- **ciscoCableAdmCtrlStatGroup** (::= { ciscoCableAdmCtrlMIBGroups 2 })—This collection of objects provides Admission Control data based on resources:
  - ccacSysRscUtilization
  - ccacSysRscMinorCrosses
  - ccacSysRscMajorCrosses
  - ccacSysRscCountersDscTime
  - ccacSysRscCriticalCrosses
  - ccacUsUtilization
  - ccacUsMinorCrosses
  - ccacUsMajorCrosses
  - ccacUsExclusiveCrosses
  - ccacUsCountersDscTime
  - ccacDsUtilization
  - ccacDsMinorCrosses
  - ccacDsMajorCrosses
  - ccacDsExclusiveCrosses
  - ccacDsCountersDscTime
- **ciscoCableAdmCtrlEventHistGroup** (::= { ciscoCableAdmCtrlMIBGroups 3 })—This collection of objects defines Admission Control event logging:
  - ccacEventHistTableSize
  - ccacEventHistLastIndex
  - ccacEventThreshObjectInstance
  - ccacEventTypeChecked
  - ccacEventResourceUtilization
  - ccacEventThreshCrosses
  - ccacEventTimeStamp

- **ciscoCableAdmCtrlNotifGroup** (::= { ciscoCableAdmCtrlMIBGroups 4 })—This notification group manages and monitors Admission Control system resources, upstream channel bandwidth, downstream bandwidth.
  - ccacNotification

MIB Capability Statements for Admission Control on the Cisco CMTS

- **CISCO-CABLE-ADM-C-CAPABILITY** imports definitions as follows:
  - MODULE-IDENTITY (from SNMPv2-SMI)
  - AGENT-CAPABILITIES (from SNMPv2-CONF)
  - ciscoAgentCapability (from CISCO-SMI)
- **ciscoCableAdmCtrlCapability** module (::= { ciscoAgentCapability 427 })—This new module provides agent capabilities for CISCO-CABLE-ADMISSION-CTR-MIB ("200412110000Z").
- **ciscoCableAdmCtrlCapability** (::= { ciscoCableAdmCtrlCapability 1 })—This V12R00 capabilities agent provides Admission Control MIB capabilities. The maximum size of the event history table is restricted to 5000. This agent supports the CISCO-CABLE-ADMISSION-CTRL-MIB, and includes the ciscoCableAdmCtrlEventHistGroup MIB object group.
  - VARIATION—ccacEventHistTableSize
  - SYNTAX—Unsigned32 (0..5000)
- ciscoCableAdmCtrlCapabilityV12R00 AGENT-CAPABILITIES ::= { ciscoCableAdmCtrlCapability 1 } —Provides Cisco Cable Admission Control MIB capabilities. This agent supports the CISCO-CABLE-ADMISSION-CTRL-MIB, and includes the ciscoCableAdmCtrlEventHistGroup MIB object group.
  - VARIATION—ccacEventHistTableSize
  - SYNTAX—Unsigned32 (0..5000)
  - DESCRIPTION—The maximum size of the event history table is presently restricted to 5000.

Object Identifiers for Admission Control MIBs

Cisco IOS release 12.3(13a)BCBC uses the following Admission Control object identifiers for the associated MIB objects:

- ciscoCableAdmCtrlMIBNotifs ::= { ciscoCableAdmCtrlMIB 0 }
- ciscoCableAdmCtrlMIBObjects ::= { ciscoCableAdmCtrlMIB 1 }
- ciscoCableAdmCtrlMIBConform ::= { ciscoCableAdmCtrlMIB 2 }
- ccacObjects ::= { ciscoCableAdmCtrlMIBObjects 1 }
- ccacConfigObjects ::= { ciscoCableAdmCtrlMIBObjects 2 }
- ccacStatObjects ::= { ciscoCableAdmCtrlMIBObjects 3 }
- ccacEventHistory ::= { ciscoCableAdmCtrlMIBObjects 4 }

Textual Conventions for Admission Control MIBs

Cisco IOS Release 12.3(13a)BCBC uses the following textual conventions for Admission Control:

- **Percent**—An integer that is in the range of a percent value.

  SYNTAX—Unsigned32 (0...100)

- **NonZeroPercent**—An integer that is in the range of a non-zero percent value.

  SYNTAX—Unsigned32 (1...100)

- **QoSServiceClassNameOrNull**—A null string or a string that represents QoS service class name. Refer to SP-RFIv1.1-I05-000714, Appendix C.2.2.3.4.

  SYNTAX—OCTET STRING (SIZE(0..15))

- **CcacMonitoredEvent**—The types of event being monitored by CMTS Admission Control:
  - **dynamicSvcFlow**—Dynamic service flow allows on-demand reservation on Layer 2 bandwidth resources.
  - **cmRegistration**—CM sends registration request to CMTS.

  The syntax bit settings are as follows:
  - **dynamicSvcFlow** = 0
  - **cmRegistration** = 1

  Refer to SP-RFIv1.1-I05-000714, Appendix C.2.2.3.3, SP-RFIv2.0-IO2-020617, Section 11.2.

- **CcacSysRscMonitoredType**—The type of system resource being monitored by the CMTS Admission Control:
  - **cpu5Sec**—The overall CPU busy percentage in the last 5 seconds period.
  - **cpu1Min**—The overall CPU busy percentage in the last 1 minute period.
  - **procMem**—The percentage of process memory which is in use
  - **ioMem**—The percentage of I/O memory which is in use.
  - **totalMem**—The percentage of memory which is in used by I/O memory and process memory.

  The syntax i ntegers are as follows:
  - **cpu5Sec** = 1
  - **cpu1Min** = 2
  - **procMem** = 3
  - **ioMem** = 4
  - **totalMem** = 5

- **CcacDSTrafficMonitoredType**—The downstream traffic type being monitored by the CMTS Admission Control:
  - **voice**—The downstream voice traffic
  - **data**—The downstream data traffic

  The syntax integers are as follows:
  - **voice** = 1
  - **data** = 2

MIB Objects in the Admission Control Group

- **ccacNotifyEnable** —(Object type) This object controls generation of notifications in the MIB. When the object is 'true', the agent generates notification defined by this MIB. When the object is 'false', the agent does not generate notification defined by this MIB. (::= { ccacObjects 1 })
  - SYNTAX—TruthValue
  - MAX-ACCESS—read-write
  - DEFVAL— false
- **ccacEventMonitoring** —(Object type) This object specifies the events being monitored by the CMTS admission control. (::= { ccacObjects 2 })
  - SYNTAX—CcacMonitoredEvent
  - MAX-ACCESS—read-write

Notifications for Admission Control

- **ccacNotification** — (Notification Type) This notification is sent when the monitoring threshold value is crossed. (::= { ciscoCableAdmCtrlMIBNotifs 1 })

  This notification contains the following objects:
  - ccacEventThreshObjectInstance
  - ccacEventTypeChecked
  - ccacEventResourceUtilization
  - ccacEventThreshCrosses

CISCO-CABLE-ADMISSION-CTRL-MIB

The CISCO-CABLE-ADMISSION-CTRL-MIB uses the following objects that are defined by other MIBs:

- MODULE-IDENTITY
- OBJECT-TYPE
- NOTIFICATION-TYPE
- Gauge32
- Unsigned32
- Counter32 (from SNMPv2-SMI)
- TEXTUAL-CONVENTION
- RowStatus
- TruthValue
- TimeStamp
- VariablePointer (from SNMPv2-TC)
- OBJECT-GROUP
- NOTIFICATION-GROUP
- MODULE-COMPLIANCE (from SNMPv2-CONF)

- ifIndex
- InterfaceIndexOrZero (from IF-MIB)
- SchedulingType (from DOCS-QOS-MIB)
- entPhysicalIndex (from ENTITY-MIB)
- ciscoMgmt (from CISCO-SMI)

ciscoCableAdmCtrlMIB Module

The ciscoCableAdmCtrlMIB module defines the managed objects for Admission Control on the Cisco CMTS. In this case, Admission Control refers to the rules that the Cisco CMTS follows when allocating and monitoring events for resources such as the following:

- CPU and memory utilization—Data and thresholds setting on the physical entity, such as the main processor or line card or BPE, when a monitoring event happens
- Upstream (US) channel bandwidth utilization—based on scheduling types or service classes
- Downstream (DS) channel bandwidth utilization—based on voice or data

The monitored events for Admission Control on the Cisco CMTS include the following:

- Dynamic service flow creation requests—Dynamic service flow allows on-demand reservation on Layer 2 bandwidth resources. CMTS can provide special QoS to the cable modem dynamically for the duration of a voice call or video session which provides a more efficient use of the available bandwidth.
- Resource requests during cable modem (CM) registration—CMTS resources are required during CM registration. CMTS resources will be checked when it receives a CM registration request.

Revision History

Table 1-10 Revision History for ciscoCableAdmCtrlMIB Module

MIB Revision Date	Cisco IOS Releases	Description
July 25, 2005 (200505040000Z)	12.3(13a)BCBC	Initial version of this MIBmodule.

MIB Module Constraints

This MIB module does not have any constraints.

MIBs and MIB Objects for PacketCable and PCMM with Admission Control

CISCO-CABLE-PACKETCABLE-MIB

The implementation for cdxQosCtrlUpTable in CISCO-DOCS-EXT-MIB continues from earlier Cisco 12.3BC releases, as 12.3(13a)BCBC continues support for this feature.

CISCO-DOCS-EXT-MIB

The CISCO-DOCS-EXT-MIB continues from earlier Cisco IOS releases, but Admission Control uses the following elements:

- cdxQosCtrlUpAdmissionCtrl
- cdxQosCtrlUpMaxRsvdBWPercent
- cdxQosCtrlUpAdmissionRejects
- cdxQosCtrlUpReservedBW
- cdxQosCtrlUpMaxVirtualBW

CISCO-CABLE-PACKETCABLE-MIB Module

Cisco IOS Release 12.3(13a)BCBC continues support for the CISCO-CABLE-PACKETCABLE-MIB, supported in prior Cisco IOS releases. In Cisco IOS Release 12.3(13a)BCBC, this MIB module supplies the basic management objects for supporting PacketCable voice traffic with Admission Control. The objects in this MIB module allow Admission Control monitoring of the following resources on the Cisco CMTS:

- CMTS CPU and memory usage
- Number of voice calls
- Various upstream throughput scheduling types
- Downstream throughput between voice and data

A trap is sent for each threshold value that is crossed.

Note The MODULE-IDENTITY for the CISCO-CABLE-PACKETCABLE-MIB is ciscoCablePktCMIB.

Note The object identifier is ciscoCablePktCMIBObjects ::= { ciscoCablePktCMIB 1 }.

Revision History

Table 1-11 Revision History for CISCO-CABLE-PACKETCABLE-MIB

MIB Revision Date	Cisco IOS Releases	Description
February 21, 2005 (200502210000Z)	12.3(13a)BCBC	Supports for these objects for Admission Control functions: • cdxQosCtrlUpAdmissionCtrl • cdxQosCtrlUpMaxRsvdBWPercent • cdxQosCtrlUpAdmissionRejects • cdxQosCtrlUpReservedBW • cdxQosCtrlUpMaxVirtualBW

Table 3-8 lists the objects and identifiers (OIDs) in the CISCO-CABLE-PACKETCABLE-MIB for Cisco CMTS routers.

Cisco DOCSIS PacketCable MIB Notifications

- **ciscoCablePktCNotificationsPrefix** (ciscoCablePktCMIB 2)
- **ciscoCablePktCNotifications** (ciscoCablePktCNotificationsPrefix 0)
- **ccpAdmCtrlSysRscNotification**—This notification is sent when the process monitoring threshold value is crossed. (ciscoCablePktCNotifications 1)
  - OBJECTS

    ccpAdmCtrlSysRscPhysicalIndex

    ccpAdmCtrlSysRscResourceType

    ccpAdmCtrlSysRscCurrentUsage

    ccpAdmCtrlSysRscMinorCt

    ccpAdmCtrlSysRscMajorCt

    ccpAdmCtrlSysRscCriticalCt

    ccpAdmCtrlSysRscLastThreshold

    TypeCrossed
- **ccpAdmCtrlUsNotification**—This notification is sent when the upstream-related threshold value is crossed. (ciscoCablePktCNotifications 2)
  - OBJECTS:

    ccpAdmCtrlUsIfIndex

    ccpAdmCtrlUsSchedType

    ccpAdmCtrlUsSrvClsIdx

    ccpAdmCtrlUsSrvClsName

    ccpAdmCtrlUsMinorThreshold

    ccpAdmCtrlUsMajorThreshold

    ccpAdmCtrlUsExclusivePercent

    ccpAdmCtrlUsMinorCt

    ccpAdmCtrlUsMajorCt

    ccpAdmCtrlUsExclusiveCt

    ccpAdmCtrlUsLastThresholdTypeCrossed
- **ccpAdmCtrlDsNotification**—This notification is sent when the downstream-related threshold value is crossed. (ciscoCablePktCNotifications 3)
  - Objects

    ccpAdmCtrlDsIfIndex

    ccpAdmCtrlDsFlowType

    ccpAdmCtrlDsMinorThreshold

    ccpAdmCtrlDsMajorThreshold

    ccpAdmCtrlDsExclusivePercent

    ccpAdmCtrlDsMinorCt

    ccpAdmCtrlDsMajorCt

    ccpAdmCtrlDsExclusiveCt

ccpAdmCtrlDsLastThresholdTypeCrossed

- ccpAdmCtrlMaxVoiceCallsNotification—This notification is sent when the number of voice calls has reached the maximum number allowed. (ciscoCablePktCNotifications 4)
  - OBJECTS:

    ccpAdmCtrlVoiceCallMaxAllowed

    ccpAdmCtrlVoiceCallCurrentNum

Admission Control Conformance Statement Object Identifiers for PacketCable

- ciscoCablePktCConformance (ciscoCablePktCMIB 3)
- ccpCablePktCGroups (ciscoCablePktCConformance 1)

MIB Objects for Configuration of CPU and Memory Resources

- **ccacSysRscConfigTable** — (Object type) This table abstracts a sparse matrix of system resource utilization thresholds to be monitored by Admission Control. (::= { ccacConfigObjects 1 })
  - SYNTAX—SEQUENCE OF CcacSysRscConfigEntry
  - MAX-ACCESS—not-accessible

  The entPhysicalIndex uniquely identifies the physical entity with a set of system resource utilization thresholds being associated. The ccacSysRscConfigResourceType identifies the system resource to be monitored.

  The physical entities, for example, processors or linecards, are being expanded upon, and the expansion entails zero or more sets of system resource utilization thresholds. The agent creates/destroys/modifies an entry whenever the local console affects this configuration.

  The management application may create/destroy/modify an entry.

  When an entry is created and ccacSysRscConfigStatus is equal to 'active', CMTS monitors the system resources based on the configurable thresholds, minor, major and critical for different monitoring system resources type and the main processor or a linecard.
- **ccacSysRscConfigEntry**— (Object type) Each entry defines a set of configurable thresholds, for each monitoring system resources type and the main processor or a linecard. (::= {ccacSysRscConfigTable 1})
  - SYNTAX—CcacSysRscConfigEntry
  - MAX-ACCESS—not-accessible
  - INDEX—{entPhysicalIndex, ccacSysRscConfigResourceType }

  CcacSysRscConfigEntry SEQUENCE:
  - ccacSysRscConfigResourceType—CcacSysRscMonitoredType
  - ccacSysRscConfigStatus—RowStatus
  - ccacSysRscConfigMinorThreshold—NonZeroPercent
  - ccacSysRscConfigMajorThreshold—NonZeroPercent
  - ccacSysRscConfigCritThreshold—NonZeroPercent

- **ccacSysRscConfigResourceType**—(Object type) This object specifies the type of system resource being monitored. (::= { ccacSysRscConfigEntry 1 })

  SYNTAX—CcacSysRscMonitoredType

  MAX-ACCESS—not-accessible

- **ccacSysRscConfigStatus**—(Object type) This object facilitates the creation, modification, and destruction of a conceptual row in this table. (::= { ccacSysRscConfigEntry 2 })
  - SYNTAX—RowStatus
  - MAX-ACCESS—read-create
- **ccacSysRscConfigMinorThreshold** —(Object type) This object specifies minor threshold settings relating to resource utilization. (::= { ccacSysRscConfigEntry 3 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create
- **ccacSysRscConfigMajorThreshold**—(Object type) This object specifies major threshold related to the utilization of the resource being monitored. The major threshold must be greater than minor threshold. (::= { ccacSysRscConfigEntry 4 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create

- **ccacSysRscConfigCritThreshold**— (Object type) This object specifies critical threshold related to the utilization of the resource being monitored. The critical threshold must be greater than major threshold. The Cisco CMTS gracefully rejects requests corresponding to monitored events if the monitored system resource exceeds the critical threshold. (::= { ccacSysRscConfigEntry 5 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create

MIB Objects for Configuration of Upstream Channel Usage

- **ccacUsConfigTable**—(Object type) This table makes a sparse matrix of upstream channel utilization thresholds to be monitored by Admission Control. (::= { ccacConfigObjects 3 })
  - SYNTAX—SEQUENCE OF CcacUsConfigEntry
  - MAX-ACCESS—not-accessible

  The ifIndex uniquely identifies all upstream channels, upstream channels associated with an interface or an upstream channel with a set of upstream channel utilization thresholds being associated.

  The ccacUsConfigSchedType identifies the scheduling type to be monitored.

  The ccacUsConfigServiceClassName identifies the cable service class to be monitored. The agent creates, destroys or modifies an entry whenever the local console affects this configuration. The management application may create, destroy or modify an entry. When an entry is created and ccacUsConfigStatus is equal to 'active', CMTS monitors the upstream channel bandwidth utilization based on the configurable thresholds, minor, major and exclusive percentage, for different scheduling type or service class for an upstream channel.
- **ccacUsConfigEntry**—(Object type) Each entry defines a set of configurable thresholds and parameters for each monitored scheduling service for an upstream channel. Scheduling service can be specified by a scheduling type or QoS Service class name. A set of thresholds applied by cable admission control in the process of monitoring upstream channel bandwidth.
  (::= {ccacUsConfigTable 1 })
  - SYNTAX—CcacUsConfigEntry
  - MAX-ACCESS—not-accessible
  - INDEX— ccacUsConfigIfIndex, ccacUsConfigSchedType, ccacUsConfigServiceClassName

  The following classes of upstream policies can be configured:
  - Global— An entry with a ccacUsConfigIfIndex of '0' identifies a global policy.
  - Per Interface—An entry with a ccacUsConfigIfIndex with an ifType of 'docsCableMaclayer' identifies an interface policy. Interface-level thresholds supersede global-level thresholds.
  - Per Upstream Channel— An entry with a ccacUsConfigIfIndex with an ifType of 'docsCableUpstream' identifies an upstream channel policy. Upstream level thresholds supersedes both global and interface level thresholds.
  - CcacUsConfigEntry SEQUENCE:

    ccacUsConfigIfIndex—InterfaceIndexOrZero

    ccacUsConfigSchedType—SchedulingType

    ccacUsConfigServiceClassName—QoSServiceClassNameOrNull

    ccacUsConfigStatus—RowStatus

ccacUsConfigMinorThreshold—NonZeroPercent

ccacUsConfigMajorThreshold—NonZeroPercent

ccacUsConfigExclusivePercent—NonZeroPercent

ccacUsConfigNonExclusivePercent—Percent

- **ccacUsConfigIfIndex** —(Object type) (::= { ccacUsConfigEntry 1 }) The object identities the interface to which the upstream channel thresholds applies:
  - If '0', then the policy applies to all upstream channels being monitored.
  - If the corresponding ifType is 'docsCableMacLayer', then the policy applies to all upstream channels being carried by the physical interface.
  - If the corresponding ifType is 'docsCableUpstream', then the policy applies to that upstream channel.
  - SYNTAX—InterfaceIndexOrZero
  - MAX-ACCESS—not-accessible
- **ccacUsConfigSchedType**—(Object type) This object specifies the scheduling type used in classifying an upstream channel. When the service class name is specified the value of this object is equal to 'undefined'. REFERENCE “SP-RFIv1.1-I05-000714, Appendix C.2.2.6.2. (::= { ccacUsConfigEntry 2 })
  - SYNTAX—SchedulingType
  - MAX-ACCESS—not-accessible
- **ccacUsConfigServiceClassName**—(Object type) This object specifies the QoS service class name. Service class name is a null string when scheduling type is specified. REFERENCE "SP-RFIv1.1-I05-000714, Appendix C.2.2.3.4.” (::= { ccacUsConfigEntry 3 })
  - SYNTAX—QoSServiceClassNameOrNull
  - MAX-ACCESS—not-accessible
- **ccacUsConfigStatus** —(Object type) This object facilitates the creation, modification, or deletion of a conceptual row in this table. (::= { ccacUsConfigEntry 4 })
  - SYNTAX—RowStatus
  - MAX-ACCESS—read-create
- **ccacUsConfigMinorThreshold**—(Object type) This object specifies the minor threshold related to the utilization of upstream bandwidth. (::= { ccacUsConfigEntry 5 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create
- **ccacUsConfigMajorThreshold**—(Object type) This object specifies the major threshold related to the utilization of upstream bandwidth. The major threshold must be greater than minor threshold. (::= { ccacUsConfigEntry 6 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create
- **ccacUsConfigExclusivePercent**—(Object type) This object specifies the reserved bandwidth exclusively related to the utilization of upstream bandwidth. The exclusive percent must be greater than major threshold. The sum of exclusive percent for all different scheduling services on this upstream channel cannot be greater than '100'. (::= { ccacUsConfigEntry 7 })
  - SYNTAX—NonZeroPercent

  - MAX-ACCESS—read-create

- **ccacUsConfigNonExclusivePercent** —(Object type) This object specifies the percentage of bandwidth, over and above the exclusive share, which can be used by scheduling service after the exclusive bandwidth has been used up. Because the bandwidth is non-exclusive, it has the potential to be shared by other classes depending on the configuration. The sum of exclusive and non-exclusive percent in the same entry cannot be greater than '100'. (::= { ccacUsConfigEntry 8 })
  - SYNTAX—Percent
  - MAX-ACCESS—read-create

MIB Objects for Configuration of Downstream Bandwidth Usage

- **ccacDsConfigTable**—(Object type) This table abstracts a sparse matrix of downstream channel utilization thresholds to be monitored by Cable Admission Control. The ifIndex uniquely identifies all downstream channels, or a downstream channel with a set of upstream channel utilization thresholds being associated. The ccacDsConfigTrafficType identifies the downstream traffic type to be monitored. The agent creates/destroys/modifies an entry whenever the local console affects this configuration. The management application may create/destroy/modify an entry. When an entry is created and ccacDsConfigStatus is equal to 'active', CMTS monitors the downstream bandwidth utilization based on the configurable thresholds, minor, major and exclusive percentage, for different traffic type for a downstream. (::= { ccacConfigObjects 4 })
  - SYNTAX—SEQUENCE OF CcacDsConfigEntry
  - MAX-ACCESS—not-accessible
- **ccacDsConfigEntry**—(Object type) Each entry defines a set of configurable thresholds and parameters for each monitoring traffic type for a downstream. A set of thresholds applied by cable admission control in the process of monitoring downstream bandwidth. (::={ccacDsConfigTable 1})
  - SYNTAX—CcacDsConfigEntry
  - MAX-ACCESS—not-accessible
  - INDEX— ccacDsConfigIfIndex, ccacDsConfigTrafficType

  The following classes of downstream policy can be configured:

  - Global— An entry with a ccacDsConfigIfIndex of '0' identifies a global policy.
  - Per Downstream Channel—An entry with a ccacDsConfigIfIndex with an ifType of 'docsCableDownstream' identifies a downstream channel policy. Downstream level thresholds supersedes global level thresholds.
  - CcacDsConfigEntry sequence:

    ccacDsConfigIfIndex—InterfaceIndexOrZero,

    ccacDsConfigTrafficType—CcacDSTrafficMonitoredType,

    ccacDsConfigStatus—RowStatus,

    ccacDsConfigMinorThreshold—NonZeroPercent,

    ccacDsConfigMajorThreshold—NonZeroPercent,

    ccacDsConfigExclusivePercent—NonZeroPercent,

    ccacDsConfigNonExclusivePercent—Percent

- **ccacDsConfigIfIndex**—(Object type) (::= { ccacDsConfigEntry 1 }) The object identities the interface to which the downstream thresholds applies:
  - If '0', then the policy applies to all downstream channels being monitored.
  - If the corresponding ifType is 'docsCableDownstream', then the policy applies to that downstream.
  - SYNTAX—InterfaceIndexOrZero
  - MAX-ACCESS—not-accessible
- **ccacDsConfigTrafficType**—(Object type) This object specifies the traffic type for which this policy applies. (::= { ccacDsConfigEntry 2 })
  - SYNTAX—CcacDSTrafficMonitoredType
  - MAX-ACCESS—not-accessible
- **ccacDsConfigStatus** —(Object type) This object facilitates the creation, modification, or deletion of a conceptual row in this table. (::= { ccacDsConfigEntry 3 })
  - SYNTAX—RowStatus
  - MAX-ACCESS—read-create
- **ccacDsConfigMinorThreshold**—(Object type) This object specifies the minor threshold related to the utilization of downstream bandwidth. (::= { ccacDsConfigEntry 4 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create
- **ccacDsConfigMajorThreshold**—(Object type) This object specifies the major threshold related to the utilization of downstream bandwidth. The major threshold must be greater than minor threshold. (::= { ccacDsConfigEntry 5 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create
- **ccacDsConfigExclusivePercent** —(Object type) This object specifies the reserved bandwidth exclusively related to the utilization of downstream bandwidth. The exclusive percent must be greater than major threshold. The sum of exclusive percent for all different traffic type on this downstream cannot be greater than '100'. (::= { ccacDsConfigEntry 6 })
  - SYNTAX—NonZeroPercent
  - MAX-ACCESS—read-create
- ccacDsConfigNonExclusivePercent—(Object type) This object specifies the percentage of bandwidth, over and above the exclusive share, which can be used by this traffic type after the exclusive bandwidth has been used up. Because the bandwidth is non-exclusive, it can be used by other traffic type as specified. The sum of exclusive and non-exclusive percent in the same entry cannot be greater than '100'. (::= { ccacDsConfigEntry 7 })
  - SYNTAX—Percent
  - MAX-ACCESS—read-create

MIB Objects for Configuration of Admission Control Event History

- **ccacEventHistTableSize**—(Object type) This object specifies the number of entries that the ccacEventHistTable can contain. When the capacity of the ccacEventHistTable has reached the value specified by this object, then the agent deletes the oldest entity in order to accommodate the new entry. A value of '0' prevents any history from being retained. (::= { ccacEventHistory 1 })
  - SYNTAX—Unsigned32
  - MAX-ACCESS—read-write
  - DEFVAL—10
- **ccacEventHistLastIndex**—(Object type) This object specifies the value of the ccacEventHistIndex object corresponding to the last entry added to the table by the agent. If the management client uses the notifications defined by this module, then it can poll this object to determine whether it has missed a notification sent by the agent. (::= { ccacEventHistory 2 })
  - SYNTAX—Unsigned32
  - MAX-ACCESS—read-only
- **ccacEventHistoryTable**—(Object type) This table contains a history of the monitored event in which the configured threshold is crossed. The number of most recent notifications is saved based on the table size. (::= { ccacEventHistory 3 })
  - SYNTAX—SEQUENCE OF CcacEventHistoryEntry
  - MAX-ACCESS—not-accessible
- **ccacEventHistoryEntry**—(Object type) The data corresponding to a monitored event in which the configured threshold is crossed. (::= { ccacEventHistoryTable 1 })
  - SYNTAX—CcacEventHistoryEntry
  - MAX-ACCESS—not-accessible
  - INDEX— ccacEventHistoryIndex
  - CcacEventHistoryEntry sequence:

    ccacEventHistoryIndex—Unsigned32

    ccacEventThreshObjectInstance—VariablePointer

    ccacEventTypeChecked—CcacMonitoredEvent

    ccacEventResourceUtilization—Unsigned32

    ccacEventThreshCrosses—Unsigned32

    ccacEventTimeStamp—TimeStamp
- **ccacEventHistoryIndex**—(Object type) An integer value uniquely identifying the entry in the table. The value of this object starts at '1' and monotonically increases for each condition transition monitored by the agent. If the value of this object is '4294967295', the agent will reset it to '1' upon monitoring the next condition transition. (::= { ccacEventHistoryEntry 1 })
  - SYNTAX—Unsigned32
  - MAX-ACCESS—not-accessible
- **ccacEventThreshObjectInstance**—(Object type) The object specifies the instance identifier of a threshold object which was crossed. (::= { ccacEventHistoryEntry 2 })
  - SYNTAX—VariablePointer
  - MAX-ACCESS—read-only

- **ccacEventTypeChecked** —(Object type) The object specifies the monitored event type when the threshold was crossed. (::= { ccacEventHistoryEntry 3 })
  - SYNTAX—CcacMonitoredEvent
  - MAX-ACCESS—read-only
- **ccacEventResourceUtilization**—(Object type) This object specifies the resource utilization when the threshold was crossed. (::= { ccacEventHistoryEntry 4 })
  - SYNTAX—Unsigned32
  - MAX-ACCESS—read-only
- **ccacEventThreshCrosses**—(Object type) This object specifies the number of times that the threshold was crossed. (::= { ccacEventHistoryEntry 5 })
  - SYNTAX—Unsigned32
  - MAX-ACCESS—read-only
- **ccacEventTimeStamp**—(Object type) This object specifies the value of the sysUpTime object at the time the notification was generated. (::= { ccacEventHistoryEntry 6 })
  - SYNTAX—TimeStamp
  - MAX-ACCESS—read-only

MIB Objects for Monitoring CPU and Memory Utilization

- **ccacSysRscTable**—(Object type) This table contains statistical data relating to system resource utilization for all configured physical entities and resource types. (::= { ccacStatObjects 1 })
  - SYNTAX—SEQUENCE OF CcacSysRscEntry
  - MAX-ACCESS—not-accessible
- **ccacSysRscEntry**—(Object type) Each entry contains objects that support monitoring of statistical data based on system resources utilization for a physical entity. (::= {ccacSysRscTable 1})
  - SYNTAX—CcacSysRscEntry
  - MAX-ACCESS—not-accessible
  - INDEX—entPhysicalIndex, ccacSysRscType
  - CcacSysRscEntry sequence:

    ccacSysRscType—CcacSysRscMonitoredType,

    ccacSysRscUtilization—Percent,

    ccacSysRscMinorCrosses—Counter32,

    ccacSysRscMajorCrosses—Counter32,

    ccacSysRscCriticalCrosses—Counter32,

    ccacSysRscCountersDscTime—TimeStamp
- **ccacSysRscType**—(Object type) This object indicates the type of system resource being monitored. (::= { ccacSysRscEntry 1 })
  - SYNTAX—CcacSysRscMonitoredType
  - MAX-ACCESS—not-accessible

- **ccacSysRscUtilization**—(Object type) This object indicates the utilization of the system resource on the physical entity. (::= { ccacSysRscEntry 2 })
  - SYNTAX—Percent
  - MAX-ACCESS—read-only
- **ccacSysRscMinorCrosses**—(Object type) This object indicates the number of times system resource utilization on the physical entity has crossed minor threshold specified by ccacSysRscConfigMinorThreshold. (::= { ccacSysRscEntry 3 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacSysRscMajorCrosses**—(Object type) This object indicates the number of times system resource utilization on the physical entity has crossed major threshold specified by ccacSysRscConfigMajorThreshold. (::= { ccacSysRscEntry 4 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacSysRscCriticalCrosses**—(Object type) This object indicates the number of times system resource utilization on the physical entity has crossed critical threshold specified by ccacSysRscConfigCritThreshold. (::= { ccacSysRscEntry 5 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacSysRscCountersDscTime**—(Object type) The value of sysUpTime on the most recent occasion at which all counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains the creation time of the corresponding counters. (::= { ccacSysRscEntry 6 })
  - SYNTAX—TimeStamp
  - MAX-ACCESS—read-only

MIB Objects for Monitoring Upstream Channel Bandwidth Utilization

- **ccacUsTable**—(Object type) This table contains statistical data relating to an upstream channel bandwidth utilization for every monitored upstream channel. There will be an entry in this table for each scheduling service per upstream channel being monitored. (::= { ccacStatObjects 3 })
  - SYNTAX—SEQUENCE OF CcacUsEntry
  - MAX-ACCESS—not-accessible
- **ccacUsEntry**—(Object type) Each entry contains statistical data relating to an upstream channel bandwidth utilization, for a scheduling service and upstream channel. (::= { ccacUsTable 1 })
  - SYNTAX—CcacUsEntry
  - MAX-ACCESS—not-accessible
  - INDEX— ifIndex, ccacUsSchedType, ccacUsServiceClassName
  - CcacUsEntry sequence:

    ccacUsSchedType—SchedulingType

    ccacUsServiceClassName—QoSServiceClassNameOrNull

    ccacUsUtilization—Percent

ccacUsMinorCrosses—Counter32

ccacUsMajorCrosses—Counter32

ccacUsExclusiveCrosses—Counter32

ccacUsCountersDscTime—TimeStamp

- **ccacUsSchedType**—(Object type) This object indicates the scheduling type of an upstream channel. When the service class name is referred the value of this object is equal to 'undefined'. REFERENCE "SP-RFIv1.1-I05-000714, Appendix C.2.2.6.2." (::= { ccacUsEntry 1 })
  - SYNTAX—SchedulingType
  - MAX-ACCESS—not-accessible
- **ccacUsServiceClassName**—(Object type) This object indicates the QoS service class name. Service class name is a null string when scheduling type is referred. REFERENCE "SP-RFIv1.1-I05-000714, Appendix C.2.2.3.4." (::= { ccacUsEntry 2 })
  - SYNTAX—QoSServiceClassNameOrNull
  - MAX-ACCESS—not-accessible
- **ccacUsUtilization**—(Object type) This object indicates the upstream channel bandwidth utilized by the scheduling service. (::= { ccacUsEntry 3 })
  - SYNTAX—Percent
  - MAX-ACCESS—read-only
- **ccacUsMinorCrosses**—(Object type) The value of the statistic during the last sampling period. This object indicates the number of times upstream channel bandwidth utilization has crossed minor threshold specified by ccacUsConfigMinorThreshold. (::= { ccacUsEntry 4 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacUsMajorCrosses**—(Object type) This object indicates the number of times upstream channel bandwidth utilization has crossed major threshold specified by ccacUsConfigMajorThreshold. (::= { ccacUsEntry 5 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacUsExclusiveCrosses**—(Object type) This object indicates the number of times upstream channel bandwidth utilization has crossed exclusive percentage specified by ccacUsConfigExclusivePercent. (::= { ccacUsEntry 6 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacUsCountersDscTime**—(Object type) The value of sysUpTime on the most recent occasion at which all counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains the creation time of the corresponding counters. (::= { ccacUsEntry 7 })
  - SYNTAX—TimeStamp
  - MAX-ACCESS—read-only

MIB Objects for Monitoring Downstream Bandwidth Utilization

- **ccacDsTable**—(Object type) This table contains the statistical data relating to downstream bandwidth utilization for every monitored downstream. There will be an entry in this table for each traffic type per downstream being monitored. (::= { ccacStatObjects 4 })
  - SYNTAX—SEQUENCE OF CcacDsEntry
  - MAX-ACCESS—not-accessible
- **ccacDsEntry**—(Object type) Each entry contains statistical data on the bandwidth utilization, per traffic type and downstream. (::= { ccacDsTable 1 })
  - SYNTAX—CcacDsEntry
  - MAX-ACCESS—not-accessible
  - INDEX { ifIndex, ccacDsTrafficType }
  - CcacDsEntry sequence:

    ccacDsTrafficType—CcacDSTrafficMonitoredType

    ccacDsUtilization—Percent

    ccacDsMinorCrosses—Counter32

    ccacDsMajorCrosses—Counter32

    ccacDsExclusiveCrosses—Counter32

    ccacDsCountersDscTime—TimeStamp
- **ccacDsTrafficType**—(Object type) This object indicates the traffic type used in classifying a downstream. (::= { ccacDsEntry 1 })
  - SYNTAX—CcacDSTrafficMonitoredType
  - MAX-ACCESS—not-accessible
- **ccacDsUtilization**—(Object type) This object indicates the downstream bandwidth utilization for the traffic type on the downstream. (::= { ccacDsEntry 2 })
  - SYNTAX—Percent
  - MAX-ACCESS—read-only
- **ccacDsMinorCrosses**—(Object type) This object indicates the number of times the minor downstream bandwidth threshold, ccacDsConfigMinorThreshold, is crossed. (::= { ccacDsEntry 3})
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacDsMajorCrosses**—(Object type) This object indicates the number of times the major downstream bandwidth threshold, ccacDsConfigMajorThreshold, is crossed. (::= {ccacDsEntry 4 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only
- **ccacDsExclusiveCrosses**—(Object type) This object indicates the number of times the exclusive percentage, ccacDsConfigExclusivePercent, is crossed. (::= { ccacDsEntry 5 })
  - SYNTAX—Counter32
  - MAX-ACCESS—read-only

- **ccacDsCountersDscTime**—(Object type) The value of sysUpTime on the most recent occasion at which all counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains the creation time of the corresponding counters. (::= {ccacDsEntry 6})
  - SYNTAX—TimeStamp
  - MAX-ACCESS—read-only

Admission Control Methods

Admission Control Dampening for CPU and Memory Resources

CPU and memory resources on the Cisco CMTS can benefit greatly by the use of a method called Admission Control dampening. Dampening is default behavior when enabling Admission Control.

Admission Control sends an alarm trap when a minor threshold value is crossed. An additional alarm trap is sent when the major threshold value is crossed. Finally, if the critical threshold value is crossed, then the call request is gracefully declined by the Cisco CMTS.

Note These minor, major, and critical threshold counters can be reset to zero by using the **clear cable admission control counters** command, and are reset to zero automatically when a given resource is reconfigured.

Dampening operates in the following manner for system CPU and memory resources. When Admission Control is configured for the first time, the system resource checks fail only if exceeding the critical threshold. Once this happens, the system resource check succeeds only if the current value is below the major threshold. This dampening method helps prevent frequent traffic spikes (when checks alternate above and below critical threshold levels).

For example, if the critical threshold is set to 80%, and the current traffic checks alternate between 79% and 81%, then without dampening, this leads to a repeating success-failure scenario. The first check succeeds, the second fails, the third check succeeds, and so forth. Automatic dampening prevents negative impact from frequently alternating success and fail checks.

Example

The following command illustrates the configuration of threshold levels on the Cisco CMTS in interface configuration mode. Dampening is achieved with this relatively normal configuration:

```
Router(config)# cable admission-control cpu-avg minor 60 major 70 critical 80 voice 200
```

This configuration implements the following Admission Control policy on the Cisco CMTS:

- When the cpu-avg threshold exceeds 60%, the Cisco CMTS sends a minor alarm.
- When the cpu-avg threshold exceeds 70%, the Cisco CMTS sends a major alarm.
- When the cpu-avg threshold exceeds 80%, the Cisco CMTS rejects the incoming request and accepts them again only after the cpu-avg threshold drops below 70% again (the major threshold level). *This is the dampening effect.*

Truth Table for Admission Control

Table 1-12 provides an illustration of collective Admission Control response to a new service request event. Admission Control responds in the following manner with either a cable modem registration (cm-registration) event or a dynamic service (voice-call) event.

Table 1-12 Illustrative Admission Control State in Response to new Service Call Event

Resource	Previous Decision (History)	Threshold(s) Crossed[1]	Current Decision
Any system resource(s)	Accept	Minor, major & critical	Reject
Any system resource(s)	Reject	Minor, major & critical	Reject
Any system resource(s)	Accept	Minor & major only	Accept
Any system resource(s)	Reject	Minor & major only	Reject
Any system resource(s)	Accept	Minor only	Accept
Any system resource(s)	Reject	Minor only	Accept
Any system resource(s)	Accept	none	Accept
Any system resource(s)	Reject	none	Accept

1. The current value here is greater than the respective CPU or memory threshold.

Additional References

The following sections provide references related to Admission Control for the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco CMTS Features Supporting Admission Control	• *Load Balancing for the Cisco CMTS* http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmtslbg.html • *Cisco CMTS MIB Specifications Guide* http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html • *DOCSIS 1.1 for the Cisco CMTS* http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html • *PacketCable and PacketCable MultiMedia for the Cisco CMTS* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm.html • *Spectrum Management for the Cisco CMTS* http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html
Cisco IOS Software for Cisco Broadband Cable	• *Cisco Broadband Cable Command Reference Guide* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html • Cisco uBR10012 Universal Broadband Router Release Notes for Cisco IOS Release 12.3(13a)BCBC http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_bulletin0900aecd80306ccc_ps2217_Products_Bulletin.html • Cisco uBR7200 Series Universal Broadband Routers Release Notes for Cisco IOS Release 12.3(13a)BCBC http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

MIBs

MIBs	MIBs Link
• MIBs introduced for Admission Control	Admission Control MIB Specifications for the Cisco CMTS
• Cisco IOS MIBs Tools	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
Technical Assistance Center (TAC) home page, containing 30,000 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