Service Group Admission Control

This document describes the Service Group Admission Control feature.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPICs DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

Restrictions for Service Group Admission Control

- To configure SGAC, the Fairness Across DOCSIS Interfaces feature must be enabled.

- SGAC supports downstream only.

Information About Service Group Admission Control

Overview

Service Group Admission Control (SGAC) is a mechanism that gracefully manages service group based admission requests when one or more resources are not available to process and support the incoming service request. Lack of such a mechanism not only causes the new request to fail with unexpected behavior but could potentially cause the flows that are in progress to have quality related problems. SGAC monitors such resources constantly, and accepts or denies requests based on resource availability.

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

Note SGAC 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.

SGAC enables you to configure 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 threshold is crossed for a given resource.

For downstream (DS) channels, you can configure the bandwidth allocation with thresholds for each fiber node.

SGAC and Downstream Bandwidth Utilization

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

Categorization of Service Flows

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

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

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

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

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

All flows use the following attribute type:

- Service class name

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

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

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

Thresholds for Downstream Bandwidth

SGAC monitors downstream bandwidth consumption using the configured maximum reserved bandwidth. It rejects service flows with a non-zero minimal rate that would make the total reserved bandwidth exceed the configured threshold.

Flexible Bandwidth Allocation

To address the issue of restricted bandwidth allocation for different application types, admission control can be applied for both normal priority and emergency voice flows. This is done by extending the threshold and assigning a group of application types in a fiber node. Each downstream service flow continues to be categorized for a single application type. However, the one-to-one mapping between an application type and a threshold no longer exists.

Each configured threshold and its associated group of application types can thus be treated as a constraint. A service flow categorized to a certain application type must pass all the constraints associated with that application type.

Overview of Bonding Group Admission Control

DOCSIS 3.0 introduced bonded channels or bonding groups that allow a single cable modem to send data over multiple RF channels achieving higher throughput. These bonding groups are defined for both upstream and downstream channels. Bonding groups are created by combining multiple RF channels. A single RF channel may also be shared by multiple bonding groups.

Note Effective from Cisco IOS-XE 3.18.0SP Release, as per DOCSIS 3.1, if bonding group contains an OFDM channel, the bonding group's total bandwidth that can be reserved (its capacity), is calculated using the least efficient OFDM profile it can use.

Bonding group SGAC functionality allows to define the maximum reserved bandwidth for an application-type as a fraction of the available bandwidth. This fraction of the bandwidth is defined as a percentage value of the total bandwidth that can be reserved.

How to Configure, Monitor, and Troubleshoot Service Group Admission Control

Configuration procedures are optional because the default configurations are enabled by default. This section presents a sequence of procedures for non-default configurations, monitoring and debugging procedures for both the default or non-default operations of SGAC.

Defining Rules for Service Flow Categorization

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

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

Note Application rules for SGAC are global configurations, and downstream bandwidth resources use the same sets of service flow rules.

Procedure

	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 application-type** *n* **include packetcable** { **normal** | **priority** } **Example:** `Router(config)# cable application-type 5 include packetcable priority`	For PacketCable, this command variation maps PacketCable service flow attributes to the specified bucket. PacketCable service flows are associated with PacketCable gates. The gate can be normal or high-priority.
Step 4	**cable application-type** *n* **include pcmm** {**priority** *gate-priority* / **app-id** *gate-app-id* } **Example:** `Router(config)# cable application-type 2 include pcmm priority 7`	For PCMM, this command variation maps PCMM service flow priority or application to the specified bucket. The PCMM gates are characterized by a priority level and by an application identifier.

	Command or Action	Purpose
	`Router(config)# cable application-type 2 include pcmm app-id 152`	
Step 5	**cable application-type** *n* **include service-class** *service-class-name* **Example:** `Router(config)# cable application-type 1 include service-class stream1`	For service class parameters, this command variation applies a service class name to the service flows, and applies corresponding QoS parameters. DOCSIS 1.1 introduced the concept of service classes. A service class is identified by a service class name. A service class name is a string that the Cisco CMTS associates with a QoS parameter set One of the objectives of using a service class is to allow the high level protocols to create service flows with the desired QoS parameter set. Using a service class is a convenient way to bind the application with the service flows. The rules provide a mechanism to implement such binding. Note the following factors when using the command in this step: • Service classes are separately configured using the **cable service class** command to define the service flow. • A named service class may be classified into any application type. • Up to ten service class names may be configured per application types. Attempting to configure more than ten service classes prints an error message. • Use the **no cable traffic-type** command to remove the configuration of a service class before adding a new class.
Step 6	**cable application-type** *n* **include BE** **Example:** `Router# cable application-type 3 include BE`	For Best Effort service flows, this command variation elaborates on Step 3, and changes the default bucket of 8 for Best Effort service flows with non-zero Committed Information Rate (CIR). These BE service flows are often created during cable modem registration.
Step 7	**Ctrl-Z** **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Example

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

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

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

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

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

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

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

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

Naming Application Buckets

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable application-type** *n***name** *bucket-name* **Example:** `Router(config)# cable application-type 7 name besteffort`	Assigns an alpha-numeric name for the specified bucket. **Note** This bucket name appears in supporting **show** and **debug** commands along with the default bucket number.
Step 4	Ctrl-Z **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Preempting High-Priority Emergency 911 Calls

You may configure SGAC rules and thresholds so that the high-priority voice (911) traffic receives an exclusive share of bandwidth. Because the average call volume for Emergency 911 traffic may not be very high, the fraction of bandwidth reserved for Emergency 911 calls may be small. In the case of regional emergency, the

call volume of Emergency 911 calls may surge. In this case, it may be necessary to preempt some of the normal voice traffic to make room for surging Emergency 911 calls.

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

SGAC preemption logic follows the following steps:

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

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

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **cable admission-control preempt priority-voice** **Example:** `Router(config)# no cable admission-control preempt priority-voice`	Changes the default Emergency 911 call preemption functions on the Cisco CMTS, supporting throughput and bandwidth requirements for Emergency 911 calls above all other buckets on the Cisco CMTS. The **no** form of this command disables this preemption, and returns the bucket that supports Emergency 911 calls to default configuration and normal function on the Cisco CMTS.

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

Calculating Bandwidth Utilization

The SGAC 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, SGAC 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.

In each of the above calculations, SGAC 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. SGAC applies a correction factor of 80% to the raw data rate to calculate the total available bandwidth.

Note For the DS and US flow in bonded channels, the maximum reserved bandwidth is the bandwidth defined for the SGAC threshold values. This value is indicated in kbps.

Enabling SGAC Check

A fiber node configured on the CMTS represents one or more matching physical fiber nodes in the HFC plant. The CMTS uses the fiber node configuration to identify the DOCSIS downstream service group (DS-SG) and DOCSIS upstream Service Group (US-SG) of the physical fiber nodes in the plant. The Service Group information is compared with MAC Domain channel configuration to automatically calculate the MAC Domain downstream and upstream service groups (MD-DS-SGs and MD-US-SGs respectively) within the MAC Domains.

Under each Fiber node, use the following procedure to enable SGAC check for an application type and any service flow of the specified application type, which is admitted to a service group.

Before you begin

Fairness Across DOCSIS Interfaces feature should always be enabled and the bandwidth percentage configured on each bonding group should be kept minimal to allow flexible adjustment of reservable bandwidth.

Restrictions

SGAC is supported only on the downstream.

SUMMARY STEPS

1. **enable**
2. **configureterminal**
3. **cable fiber-node** *id*
4. **admission-control application-type** *n* **ds-bandwidth** *pct*
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	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable fiber-node** *id* **Example:** `Router(config)# cable fiber-node 1`	Enters cable fiber-node configuration mode to configure a fiber node.
Step 4	**admission-control application-type** *n* **ds-bandwidth** *pct* **Example:** `Router(config-fiber-node)# admission-control application-type 1 ds-bandwidth 1`	Enables SGAC checking for the specified application-type. Use the **no** form of this command to disable SGAC checking.
Step 5	Ctrl-Z **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to do next

Use the **show cable admission-control fiber-node** *n* command to verify admission-control configuration.

Configuration Examples for SGAC

This section describes solutions-level examples of the SGAC feature on the Cisco CMTS. This section illustrates the functioning of SGAC in default or non-default operational configurations.

Example: SGAC Configuration Commands

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

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

The following configuration commands enable these settings:

- To map the packetcable voice flows, use:

```
cable application-type 1 include packetcable normal
```

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

- To map the BE flows into bucket 8, use:

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

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

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

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

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

```
Router# show cable admission-control fiber-node 1
App-type    Name       Exclusive
1                      N/A
2                      N/A
3           Normal     10%
4                      N/A
5                      N/A
6                      N/A
7           Emergency  N/A
8                      N/A
```

```
Router#show cable admission-control interface integrated-Cable 8/0/0:0

Interface In8/0/0:0
RFID 24576

Resource - Downstream Bandwidth
-------------------------------
App-type    Name       Reservation/bps    Exclusive      Rejected
1                      0                  N/A            0
2                      0                  N/A            0
3           Normal     0                  10%            0
4                      0                  N/A            0
5                      0                  N/A            0
6                      0                  N/A            0
7           Emergency  0                  N/A            0
8                      0                  N/A            0
Max Reserved BW = 300000 bps
Total Current Reservation = 0 bps
```

```
Guaranteed Bonus BW = 21055000 bps
Non-guaranteed Bonus BW = 7744000 bps
Superset BGs: Wi8/0/0:0 Wi8/0/0:4 Wi8/0/0:6


Router#show cable admission-control interface wideband-Cable 8/0/0:0

Interface Wi8/0/0:0
BGID: 24577

Resource - Downstream Bandwidth
-------------------------------
App-type    Name       Reservation/bps    Exclusive      Rejected
1                      0                  N/A            0
2                      0                  N/A            0
3           Normal     0                  10%            0
4                      0                  N/A            0
5                      0                  N/A            0
6                      0                  N/A            0
7           Emergency  0                  N/A            0
8                      0                  N/A            0
Max Reserved BW = 600000 bps
Total Current Reservation = 0 bps
Guaranteed Bonus BW = 21055000 bps
Non-guaranteed Bonus BW = 36844000 bps
Subset BGs: In8/0/0:0 In8/0/0:1
Superset BGs: Wi8/0/0:4 Wi8/0/0:6
Overlapping BGs: N/A
```

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

Example: SGAC for Downstream Traffic

This example presumes that you have configured the rules according to the commands illustrated at the start of this section.

- All the voice flows in bucket 1.
- All the CIR data flows are categorized in bucket 8.

The below example illustrates a sample configuration for SGAC 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.

The following command implements this configuration:

```
Router(config-fiber-node)#admission-control application-type 1 ds-bandwidth 30
```

The below example illustrates how flexible bandwidth allocation is configured. In this example, normal voice traffic (application-type 1) is associated with two thresholds. Normal voice traffic alone can use up to 40% of the service group's capacity, while normal and emergency voice traffic combined can use up to 50% of the service group’s capacity. This means that emergency voice traffic can have at least 10% of the service group's capacity, even if normal voice traffic has used up its share of 40%:

```
Router(config-fiber-node)#admission-control application-type 1 ds-bandwidth 40
Router(config-fiber-node)#admission-control application-type 1-2 ds-bandwidth 50
```

where,

- 1 is normal voice application type
- 2 is emergency voice application type

Additional References

The following topics provide references related to SGAC for the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco CMTS Cable Commands	Cisco CMTS Cable Command Reference

Standards

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

MIBs

MIB	MIBs Link
MIBs	To locate and download MIBs for selected platforms, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature Information for Service Group Admission Control

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for Service Group Admission Control

Feature Name	Releases	Feature Information
Service group admission control	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on Cisco cBR Series Converged Broadband Routers.