

CISCO SERVICE CONTROL SOLUTION GUIDE



Cisco Service Control Traffic Optimization:

Capacity Control Solution Guide, SCE 8000, Release 5.1.x

- 1 Introduction and Toolset Overview
- **2** Configuring the Solution
- **3** Obtaining Documentation and Submitting a Service Request



This document supports all 5.1.x releases.

1 Introduction and Toolset Overview

Introduction

Delivering a quality broadband experience is increasingly difficult with the demand on the available network capacity, delay-sensitive applications, and a subscriber base that is sensitive to privacy, neutrality, and fairness. Service providers face exponential growth in the demand for network resources, which is driven by new applications built to consume as much bandwidth as possible. Adding more capacity to the network provides only temporary relief because it is quickly consumed by the applications. Moreover, it is an additional expense to the service provider. Additionally, new delay-sensitive applications such as VoIP are severely affected by the congestion events caused by the high load of the network. This affects user experience and reduces subscriber satisfaction.

The Cisco Service Control Engine (Cisco SCE) provides a toolset to deal with such challenges. The Cisco SCE network management controls the network capacity, while increasing the provider revenue. The Cisco SCE enables you to create policies that are customized to your business. You can actively prioritize specific subscribers or specific applications, and create incentives for subscribers to upgrade their plans to higher subscription plans.

Cisco SCE Capacity Control Solution

The Cisco SCE Capacity Control Solution deals with the demand for network resources. This demand is driven by the presence of applications that consume as much bandwidth as possible and the coexistence of delay-sensitive applications that are badly affected by the congestion caused by these high-bandwidth consumption applications. The goal of this solution is to divide the available network resources fairly between all active subscribers, while maximizing the overall experience of all the subscribers using the network.

Using this solution, you can configure the Cisco SCE to work in one of two ways:

- Anonymous subscriber mode—The Cisco SCE is aware of the individual subscribers using the network.
- Subscriberless mode—The Cisco SCE controls each session individually without looking at the context of the subscriber.

In anonymous subscriber mode, there is no need to integrate the Cisco SCE with the operations support systems (OSS). In anonymous subscriber mode, the Cisco SCE automatically defines each IP address as a subscriber and when the network is congested, the Cisco SCE fairly divides the resources between the subscribers. When the Cisco SCE is working in subscriberless mode, the bandwidth is fairly shared between the individual sessions, but not between the subscribers.

In the Capacity Control solution, the Cisco SCE enforces the policy only when one of the network resources, such as the physical interface of the Cisco SCE, is congested. However, you can set additional rules that create congestion. For example, you can limit the total bandwidth that is allocated for a specific application. When the total bandwidth from the specific application exceeds the predefined rule, the system enforces the policy to fairly share the resources of this application between all subscribers using the application.

To maximize the overall experience of all subscribers using the network, you can prioritize specific applications when congestion occurs instead of statically limiting the total bandwidth of specific applications. The Cisco SCE provides 10 levels of hierarchy and you can set each application to one of these levels. When there is congestion, traffic from level 1 is affected first. If the congestion continues, level 2 is affected, and so on. Traffic from level 10 is never affected, allowing you to mark specific applications as untouched by the Cisco SCE under any condition.

Cisco SCE Tiered Services Solution

The Cisco SCE Tiered Services Solution provides a toolset with which to increase revenue by applying policies that prioritize specific subscribers or services. Where the Capacity Control solution fairly allocates the bandwidth between all subscribers, the Tiered Services Solution provides an infrastructure for differentiating between subscribers to achieve your business goals.

The tiered services are used to create several profiles called packages. Each package contains multiple features that can be customized. Features include:

- Limiting the maximum bandwidth
- Minimizing the bandwidth allocated first in priority
- Assigning the relative hierarchy level that defines the portion of bandwidth that a package receives during congestion

In addition, each package includes a set of rules for specific applications, which are either allowed or blocked in the package, the sharing of the bandwidth of a subscriber between multiple applications, the priority between the services, and so on.

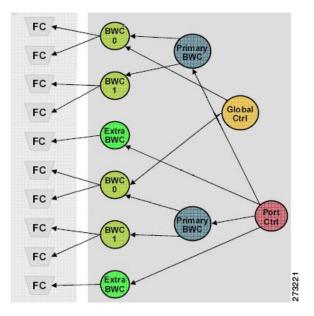
The Tiered Services Solution always includes integration of the Cisco SCE with your OSS so that you can identify and apply the correct policies for the subscribers.

Cisco SCE Toolset Overview

The physical link bandwidth is an absolute limit on the bandwidth that travels through the system (see Figure 1). To optimize traffic, you can limit the available bandwidth on two levels:

- Subscriber bandwidth control-Limits the available bandwidth per subscriber
- Global control—Limits the available bandwidth per service
- The Capacity Control solution consists of these configurable building blocks:
- Bandwidth Controller (BWC)—Controls the available bandwidth per service, per subscriber
- Primary Bandwidth Controllers (PBWC)—Controls the total traffic per subscriber
- Global Controllers-Controls the total bandwidth per service, per group of subscribers
- Port Controller-Controls the total bandwidth of the physical port on the Cisco SCE

Figure 1 Bandwidth Management Building Blocks



Bandwidth Control

Subscriber BWCs control the bandwidth from a specific service used by individual subscribers. Each BWC controls available bandwidth for selected services.

A BWC is specified by these parameters:

- Committed information rate (CIR)-Minimum bandwidth that is granted to the services controlled by the BWC.
- Peak information rate (PIR)-Maximum bandwidth that the services controlled by the BWC can consume.

• Assurance Level (AL)—Rate of change of available bandwidth under conditions of traffic congestion.

The AL controls how quickly the bandwidth of the service decreases from the PIR to the CIR as congestion builds, or how quickly the actual information rate (AIR) increases from the CIR to the PIR as congestion decreases.

The BWC ensures that even when the network is congested (PIR congestion), at least the CIR is granted. Similarly, the BWC ensures that even when there is little traffic associated with a BWC, the PIR is not exceeded.

Bandwidth may be thought of in terms of a virtual pipe of adjustable width. The PIR is the maximum allowed width of the virtual pipe. The CIR is the minimum width to which the pipe can contract. The actual pipe width is between the CIR and the AIR. During network congestion, the system contracts each pipe differently to differentiate between subscribers and between their services.

Primary and Service Bandwidth Control

In the Cisco Service Control Application for Broadband (Cisco SCA BB), each subscriber has an independent set of BWCs, consisting of a single Primary BWC that controls the total bandwidth available to the subscriber and several Service BWCs that control the available bandwidth of some services of that subscriber. For example, one BWC may control the streaming service; another may control the download and e-mail services together.

The PIR defines the maximum bandwidth for the associated services; the CIR defines the minimum bandwidth for the services.

External Bandwidth Control

An external bandwidth controller (EBC) controls the available bandwidth for a specific service negating the defined subscriber parameters. For example, the EBC may control VoIP to ensure that it always has sufficient bandwidth regardless of the other subscriber parameters.

Global Bandwidth Control

Global controllers provide constraints for large, global volumes of traffic, such as Total Gold Subscriber Traffic, or Total P2P Traffic. Each global controller defines the maximum bandwidth allowed for a particular type. Using a global controller, you can limit the total traffic of services in the system, such as Peer-to-Peer (P2P), to any desired bandwidth.

Port Control

The physical link bandwidth is an absolute limit on the bandwidth that can pass through the system. You can limit the total bandwidth capacity of the Cisco SCE platform to a value lower than the physical link bandwidth. For example, if another device connected to the Cisco SCE platform on the IP stream has limited bandwidth capacity, you can limit the bandwidth passing through the Cisco SCE platform to match the capacity of the other device.

2 Configuring the Solution

This chapter describes these solutions for local links as well as the steps to configure them:

- Capacity Control, page 4
- Tiered Subscriber Services, page 14
- Capacity Control and Tiered Subscriber Services, page 21

Capacity Control

The Capacity Control solution provides a means to distribute the total amount of bandwidth equally over the local links.

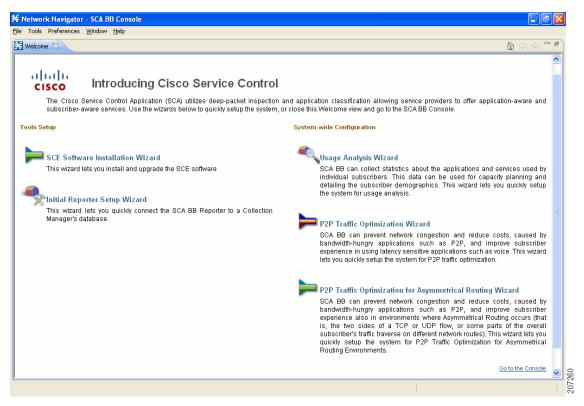
Cisco SCA BB supports theses two modes in which the Capacity Control solution can be configured:

- Subscriberless mode—Available bandwidth is divided equally between the flows. This means that the same amount of bandwidth is allocated per service regardless of the number of services each subscriber is currently running.
- Anonymous subscriber mode—Available bandwidth is divided equally between subscribers. The total bandwidth of each subscriber is then divided equally between their services. This means that all subscribers have an equal amount of bandwidth regardless of the number of services they are running.

Configuring the Capacity Control Solution

Step 1 From the Cisco SCA BB Console main menu, choose Help > Welcome. The Welcome window appears (see Figure 2).

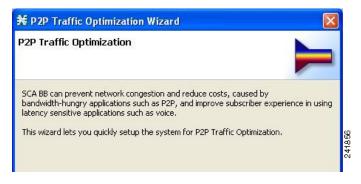
Figure 2 Welcome Window



Step 2 Click **P2P** Traffic Optimization Wizard.

The Welcome window of the P2P Traffic Optimization wizard appears (see Figure 3).







You can also open the P2P Traffic Optimization wizard from the Network Navigator tool:
1. Select one or more devices in the Site Manager tree.
2. Right-click one of the selected devices. A popup menu appears.
3. Choose Configuration Wizards > P2P Traffic Optimization Wizard.
You can set only one Cisco Service Control Collection Manager in the wizard. If you select more than one Cisco Service Control Collection Manager, only one Collection Manager is selected and a warning message is displayed.
5. Click OK to continue.

Step 3 Click Next.

The Cisco SCE IP Addresses window of the P2P Traffic Optimization wizard appears (see Figure 4).

Figure 4 Cisco SCE IP Addresses Window

€ P2P Traffic C	ptimization	Wizard			
CE IP Address	es				
One or more SC	E IP addresses n	nust be specifi	ed		
Configuring the SCE Navigator.	: platforms requi	res that they	are first added (to the Network	
To add SCE platforr box below (For exa				dresses in the t	æxt
					~
					~
	7	-			
	< <u>B</u> ack	Next >	Einish	Car	ncel

Step 4 Enter the IP addresses of the Cisco SCE devices to be added to the model.

If you started from Network Navigator, the IP addresses of the Cisco SCE devices that you selected are displayed. You can add additional addresses.



You can work with up to 20 Cisco SCE devices at one time using the wizard.

Step 5 Click Next.

The Cisco SCE Usernames and Passwords window of the P2P Traffic Optimization wizard appears (see Figure 5).

Figure 5 Cisco SCE Usernames and Passwords Window

其 P2P Tra	affic Optimization Wizard	×
	ames and Passwords ord for the SCE 10.56.216.37 is missing	
specified fo	connect to the SCE platforms, a username and a password need to be r each SCE. mmon username and a common password for all SCE platforms:	
<u>U</u> sername:	admin	
Password:		
SCE IP Ad		

Step 6 Enter the username and password for the Cisco SCE devices.

Do one of these:

- To use the same username and password for all the Cisco SCE devices that you are adding, enter the username in the Username field and the password in the Password field.
- To provide a different username and password pair for each Cisco SCE device, click the Use separate usernames and passwords for each Cisco SCE platform radio button, and, for each Cisco SCE device, enter the username and password in the appropriate cell of the Cisco SCE device table.

Step 7 Click Next.

The CM Setup window of the P2P Traffic Optimization wizard appears (see Figure 6).

Figure 6 CM Setup Window

关 P2P Traffic	Optimization Wizard
CM Setup	
🔕 An IP address	is missing
CM to the Networ boxes below. The wizard will ve	M requires that it is first added to the Network Navigator. To add the & Navigator, type its IP address, username and password in the text wify the CM operational state, and configure the SCE platfroms to CM. You may skip this step if the CM is already defined as the RDR sCE platforms.
Skip this step	
CM <u>I</u> P address:	×
CM <u>u</u> sername:	scmscm
CM <u>p</u> assword:	
	< <u>B</u> ack Next > Einish Cancel

Step 8 Define the Cisco Service Control Collection Manager to use with this configuration.

Do one of these:

• Enter the IP address, username, and password of the Cisco Service Control Collection Manager device in the appropriate fields.

If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

• Check the Skip this step check box.

Step 9 Click Next.

The Connectivity Test window of the P2P Traffic Optimization wizard appears (see Figure 7). The wizard tests the connectivity between the defined devices.

Figure 7 Connectivity Test Window

¥ SCE	Software Up	grade Wizard	
	c tivity Test connectivity		1
that cor Please v In case correct	rect IP address vait for the conr of an error, you the IP addresse	es, usernames and passworn nectivity test to complete. 1 may use the 'Back' button (to go back to previous steps and , if necessary. You may also choose
Туре	IP Address	Status	
SCE	10.10.10.10	Connection succeeded	
Ser	10.10.10.20	Connection succeeded	
Skip c	onnectivity test	Retry connectivity test	
	(< Back Next >	Finish Cancel

If a connection to one or more of the devices cannot be made, or if there is some problem with the connection (such as invalid version of the device), an error is displayed next to the device. You can skip these tests by clicking **Skip connectivity test**. The connections are validated when you click Finish at the end of the wizard.

Step 10 Click Next.

The Anonymous Subscribers window of the P2P Traffic Optimization wizard appears (see Figure 8).

Figure 8 Anonymous Subscribers Window

¥ P2P Traffic Optimization Wizard 🛛 🛛 🛛
Processing traffic per individual subscriber's IP address in Anonymous Subscribers Mode
In Anonymous Subscribers mode, analysis is performed on an incoming IP address, as the SCE platform creates an 'anonymous', on-the-fly record for each subscriber. This permits analyzing and controlling traffic at an individual subscriber IP address level, without OSS integration. You may choose to skip this step if other form of subscriber integration is already configured in the system. ▼ Enable Anonymous Subscribers mode
< <u>Back</u> <u>Next</u> Einish Cancel

- **Step 11** Check the Enable Anonymous Subscribers mode check box, to configure the Cisco SCE to work in anonymous subscriber mode. To configure the Cisco SCE to work in subscriberless mode, uncheck the Enable Anonymous Subscribers mode check box.
- Step 12 Click Next.

The effect of P2P traffic optimization window of the P2P Traffic Optimization wizard appears (see Figure 9), which explains why you should optimize (limit) peer-to-peer (P2P) traffic.

Figure 9 Effect of P2P Traffic Optimization Window

The effect of P2	P traffic optimization
High (voice), Mediur The two charts belo the left shows how, (total traffic crosses deteriorates. The prioritization th traffic rate crosses	es the system to enforce strict priority between 3 levels of service: n (other) and Low (P2P). w demonstrate the effect of P2P traffic optimization. The chart on during peak hours, uncontrolled P2P (in blue) causes congestion the red line), while browsing (yellow) and voice (green) quality at is enforced by this configuration takes place when the total the configured limit. The chart on the right shows how congestion is ng P2P traffic, while allowing browsing and voice traffic to take its $ \underbrace{\begin{array}{c} \hline \hline $
	<back next=""> Einish Cancel</back>

Step 13 Click Next.

The Link rate limits for P2P traffic optimization window of the P2P Traffic Optimization wizard appears (see Figure 10).

Figure 10 Link Rate Limits for P2P Traffic Optimization Window

🗲 P2P Traffic Optimization Wizard 🛛 🛛 🔯				
Link rate limits for P2P traffic optimization				
(the red line) that s	, configure the total upstream and downstrea should be enforced by the SCE platform. The S does not exceed this configuration, while mai applications.	iCE platform will make		
These settings can	be changed later in the Global Controllers con	figuration dialog.		
<u>U</u> pstream limit:	30% (60	0Mbps of 2Gbps)		
<u>D</u> ownstream limit:	100% (2	Gbps of 2Gbps)		
	< Back Next > Einist	Cancel		

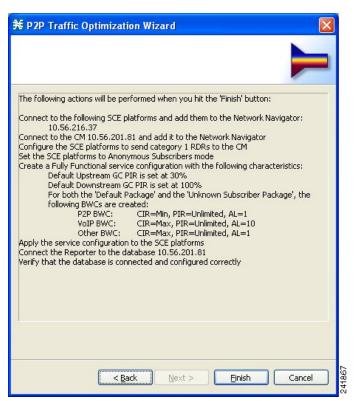
Step 14 Configure the upstream and downstream link rate limits by using the sliders.

The scale of each slider is the percentage of the aggregated bandwidth of both links.

Step 15 Click Next.

The Confirmation window of the P2P Traffic Optimization wizard appears (see Figure 11).

Figure 11 Confirmation Window



The actions that the wizard is about to take are listed in the window.

Step 16 Click Finish.

The Configuration Output window of the P2P Traffic Optimization wizard appears (see Figure 12).

Figure 12 Configuration Output Window

¥ Configuration Output
Configuration Output
Please wait while the system is being configured.
<pre>11/28/13 12:31:11 PM IST INFO Adding devices to the Network Navigator 11/28/13 12:31:11 PM IST INFO Connecting to SCE 10.78.241.210 11/28/13 12:31:11 PM IST INFO Verifying that the SCE platforms are installed properly 11/28/13 12:31:11 PM IST INFO Verifying that the CM is installed properly 11/28/13 12:31:15 PM IST INFO Verifying that the CM is installed properly 11/28/13 12:31:16 PM IST INFO Applying configuration to SCE 10.78.241.210 (1 out of 1 SCE platforms) 11/28/13 12:31:18 PM IST INFO Applying configuration to SCE 10.78.241.210 (1 out of 1 SCE platforms) 11/28/13 12:31:18 PM IST INFO System mode changed to Full Functionality 11/28/13 12:31:18 PM IST INFO System mode changed to Full Functionality 11/28/13 12:31:20 PM IST INFO System configuration to SCE 11/28/13 12:31:25 PM IST INFO Sending configuration to SCE 11/28/13 12:31:25 PM IST INFO Executing configuration to SCE 11/28/13 12:32:39 PM IST INFO Updating configuration registry 11/28/13 12:32:40 PM IST INFO Updating configuration to SCE 11/28/13 12:32:48 PM IST INFO Updating server at 10.78.242.219 with service configuration values 11/28/13 12:32:48 PM IST INFO Updating the Server at 10.78.242.219 completed successfully 11/28/13 12:32:48 PM IST INFO Updating the Server at 10.78.242.219 completed. 11/28/13 12:32:48 PM IST INFO Updating the Server at 10.78.242.219 completed.</pre>
<
Close Cancel

New devices are added to the default site of the Site Manager tree in the Network Navigator (see Figure 13).

Figure 13 Network Navigator – Site Manager Tree

🕈 Network Navigator 🗙	
🖃 🔝 Site Manager	
🖮 🚠 default site	
- 薞 SCE device 1 [10.78.241.206]	
- 💽 SM device [1.0.2.217]	
	61639
	6

The wizard attempts to connect to all devices that you defined. The operation fails if:

- The wizard cannot connect to any of the Cisco SCE devices that you listed in Step 4.
- You defined a Collection Manager in Step 8, but the wizard cannot connect to it.

If you defined a Collection Manager in Step 8, the Cisco SCE devices are configured so that the only category 1 Raw Data Record (RDR) destination is the Collection Manager.



RDR categories are the mechanism by which different types of RDRs can be sent to different collectors. For details about RDR categories, see the *Cisco Service Control Application for Broadband Reference Guide*.

A new service configuration named P2P Traffic Optimization is created, and opens in the Service Configuration Editor. The new service configuration has these characteristics:

- The Full Functionality mode is active.
- The upstream and downstream default AGCs are set with the link limit values defined in Step 13.
- For both the default package and the Unknown Subscriber Traffic package, the following upstream and downstream BWCs are created:

Table 1 BWCs for Default and Unknown Subscriber Traffic Packages

Packages	CIR	PIR	AL
P2P	0	<value controller="" global="" in="" set=""></value>	1
VoIP	<value controller="" global="" in="" set=""></value>	<value controller="" global="" in="" set=""></value>	10
P2P	<value controller="" global="" in="" set=""></value>	<value controller="" global="" in="" set=""></value>	1

The service configuration is applied to the Cisco SCE devices.

Step 17 Click Finish.

The P2P Traffic Optimization wizard closes.

Tiered Subscriber Services

The Tiered Subscriber Services solution enables you to create different subscriber packages with class of service parameters defined for each package.

Within each package, you define the available bandwidth and allotted services, as well as the priorities for the selected services. Additionally, you can define priorities between the packages so that when the link is congested, each package receives a different, predefined share of the bandwidth.

For example, you can define these three packages:

• Gold—5 MB, three services (VoIP, P2P, browsing)

- Silver—3 MB, three services (VoIP, browsing, P2P)
- Bronze—1.5 MB, two services (browsing and P2P)

In this example, you give priority to the VoIP of the silver package so that if all services are running simultaneously, VoIP still has sufficient bandwidth for optimal performance.

Gold has top priority, followed by silver, and then bronze. When the link is congested, gold has the most available bandwidth followed by silver, and then bronze.

Configuring the Tiered Subscriber Services Solution

- **Step 1** Create a new service configuration file.
 - a. In the Service Configuration Editor tool, from the Console main menu, choose File > New Service Configuration. The New Service Configuration Settings window appears (see Figure 14).

Figure 14 New Service Configuration Settings Window

New Service Configuration Settings
System Operational Mode
Select the system's operational mode for handling the network traffic:
O Transparent
Report Only
O Full Functionality
Routing Classification Mode Enable Asymmetric Routing Classification Mode in topologies with high rate of unidirectional flows. In this mode, the system is better tuned for classifying traffic according to just one side of the flow, but some control capabilities are disabled. Enable the Asymmetric Routing Classification Mode
QK Cancel

- b. In the System Operational Mode area, click the Full Functionality radio button.
- c. Click OK.

The new service configuration is added to the Console window, open on the Policies tab, and becomes the active service configuration (see Figure 15).

¥ Service Configuration Editor - <new service configuration> - SCA BB Console File Tools Preferences Window Help 📑 😂 🔡 🗄 🌺 😰 🤡 Service Configuration Editor 😁 Network Navigator - 8 🤡 <new service configuration> 🔀 Policies : Subscriber Policies : Default Package 🛃 Policies 🛛 📃 Classification 5 ÷ ж 1 Default Package : Default Service 💠 🕂 🗶 🔪 Configuration 🗸 Rule Action 🐨 Filtered Traffic controlled 🐔 Default Rule 👆 Service Security Global Policy Default Package Unknown Subscriber Traffic 📃 Console 🛃 Problems 🖳 🚮 🛛 🛫 🖽 👻 📬 🕶 Console Report Only

Figure 15 Service Configuration Editor – New Service Configuration

Step 2 Add a new package.

 a. In the Policies tab, click Subscriber policies, and click the Add Package (+) icon. The Package Settings window appears (see Figure 16).

Figure 16 Package Settings Window

Package	e Settings for ""			
General	Quota Management	Subscriber BW Controllers	Advanced	
	je <u>n</u> ame:			
Packa				
Descrip	otion:			
				QK <u>Cancel</u>

- **b**. In the **Package name** field, enter Gold.
- c. In the Description field, enter a meaningful description for the Gold package.
- d. Click OK.
- **Step 3** Add these services to the Gold package:
 - Voice and Video Calls
 - P2P
 - Browsing
 - **a**. Click the Gold package.
 - b. In the right (Rule) pane, click the add rule (+) icon.
 The Add New Rule to Package window appears (see Figure 17).

Figure 17 Add New Rule to Package Window

Add Ne	ew Ru	le to Packag	ge "Gold"				×
General	Iontrol	Usage Limits	Breach Handling				
Service		ionuico to urbid	n the Rule will relate]
Oth						 ~	
-Rule St							
		state of this Ru reporting and					
		reporting and					
]
?				C	ОК	Cancel	

- c. In the Service area, from the Select the Service to which the Rule will relate drop-down list, choose Voice and Video Calls.
- d. Click OK.
- e. Repeat Steps a to d, adding P2P and Browsing services.
- Step 4 For each service, create an upstream and downstream BWC and configure the BWC parameters.
 - a. Click the Gold package, and click the edit (<u>)</u> icon.
 The Package Settings dialog box appears.
 - In the Package Settings dialog box, click the Subscriber BW Controllers tab. The Subscriber BW Controllers tab appears (see Figure 18).

Figure 18 Subscriber BW Controllers Tab

🛠 Package Settings for "Default	Package"					
General Quota Management Subscribe	er BW Controlle	rs Advanced				
Subscriber BW Controllers limit the BW o for a single subscriber. They are also us				f diffe	rent se	rvices
Upstream Subscriber relative priority (upstream)	: 5 🖌			0	œ	×
Name	CIR (L3 K	PIR (L3 K	Global Controller		AL	
🖃 🛥 Primary Upstream BWC	0	Unlimited				
🦶 🛲 Default Upstream BWC	0	Unlimited	Default Global Controller	:	l	
Downstream Subscriber relative priority (downstrea	m): 5 💌			0	¢	×
Name	CIR (L3 K	PIR (L3 K	Global Controller		AL	
📃 👄 Primary Downstream BWC	0	Unlimited				
E Default Downstream BWC	0	Unlimited	Default Global Controller		1	
0			ОК		Ca	ncel

- **c.** Add an upstream BWC to the package. In the Upstream area, click the add sub BWC () icon. A new BWC is added.
- d. In the Name field, enter Upstream Voice and Video Calls.
- e. Configure the parameters for the BWC, as required for the Voice and Video Calls service, as follows:
 - In the CIR (Kbps) field, enter 256.
 - In the PIR (Kbps) field, enter Unlimited.
 - In the AL field drop-down list, choose 9.
- f. Add a downstream BWC, and configure the parameters, as required for the Voice and Video Calls service, as follows:
 - In the Name field, enter Downstream Voice and Video Calls.
 - In the CIR (Kbps) field, enter 256.
 - In the PIR (Kbps) field, enter Unlimited.
 - In the AL field drop-down list, choose 9.
- g. Configure the remaining BWCs with the values displayed in the window in Figure 19.

Figure 19 Package Settings Example

Jpstream Subscriber relative priority (upstre	am): 9	*					0	Ø	×
Name		CIR (L	.3	PIR (L3		Global Controller		AL	
Primary Upstream BWC		0		nlimited					
Default Upstream BWC		0	U	nlimited	1	Default Global Controller		1	
- Dpstream Voice and Vic	leo Calls	256	U	nlimited	1	Default Global Controller		9	
		256	1	024		Default Global Controller		1	
		0		nlimited	J	Default Global Controller		5	~
	tream):]	perault Global Controller	0	ر ج	×
Subscriber relative priority (downs			PIR (l	L3	-	perault Global Controller	() AL	O	×
ownstream Subscriber relative priority (downs Name Primary Downstream BWC		9 🗸	PIR (L	L3	Glot	Dal Controller		Ŷ	×
Subscriber relative priority (downs Name 		9 🗸	PIR (l Unlimite Unlimite	L3 ed [Glot	bal Controller ult Global Controller	1	œ	×
Subscriber relative priority (downs Name 	CIF 0 WC 0 Vide256	9 🗸	PIR (l Unlimite Unlimite	L3 ed ed [ed [Glot Defa	oal Controller ult Global Controller ult Global Controller	1 9	Ø	*
Subscriber relative priority (downs Name Primary Downstream BWC Default Downstream BV Downstream Voice and Downstream P2P	CIF 0 WC 0 Vid: 256 256	9 🗸	PIR (I Unlimite Unlimite 5000	L3 ed ed [ed [Glot Defa Defa	oal Controller ult Global Controller ult Global Controller ult Global Controller	1 9 1	¢	*
Downstream Subscriber relative priority (downs Name Image: Primary Downstream BWC Image: Default Downstream BWC Image: Downstream Voice and	CIF 0 WC 0 Vide256	9 🗸	PIR (l Unlimite Unlimite	L3 ed ed [ed [Glot Defa Defa	oal Controller ult Global Controller ult Global Controller	1 9	©	*

h. From the Subscriber relative priority drop-down list (for both upstream and downstream), choose 9.

Step 5 Associate the services with the BWCs.

- a. Click the Voice and Video Calls rule, and click the edit () icon.
 The Add New Rule for Service dialog box appears.
- **b.** Click the **Control** tab.

The Control tab opens (see Figure 20).

Figure 20 Control Tab

🗚 Edit Rule for Service "Voice and Video Calls"	×
General Control Usage Limits Breach Handling	
Define the per-flow action to be performed by this Rule:	
O Block the flow	
Control the flow's characteristics:	
Select an upstream Bandwidth Controller Default Upstream BWC	
Select a downstream Bandwidth Controller Default Downstream BWC	
Limit the flow's upstream bandwidth to	
Limit the flow's downstream bandwidth to Kbps	
Set the flow's upstream packets ToS (DSCP) to ToS 1 [0]	
Set the flow's downstream packets ToS (DSCP) to ToS 1 [0]	
Limit concurrent flows of this Service to	
Set CoS for flows of this Service to BE	
Redirect profile for this service: Default Redirection	
Mirror traffic to server group: Server Group 0	
OK Cancel	

- c. From the Select an upstream Bandwidth Controller drop-down list, choose Upstream Voice and Video Calls.
- d. From the Select a downstream Bandwidth Controller drop-down list, choose Downstream Voice and Video Calls.
- e. Click OK.
- f. Repeat Steps a to e for the other services.
- **Step 6** Duplicate the Gold Package and apply required changes to create a Silver package.
 - a. Click the Gold package, and click the duplicate package (⁴/₄) icon.
 A duplicate package is created with all the same attributes as the original package. The name of the new package is *Gold (1)*.
 - **b.** Click the Gold (1) package and click the edit (**\)** icon.
 - c. In the Name field, enter Silver and enter an appropriate description in the Description field.
 - **d**. Change the BWCs to reflect the Silver configurations.
- **Step 7** Repeat Step 6 to create a Bronze package.

Capacity Control and Tiered Subscriber Services

The Capacity Control and Tiered Subscriber Services solution is a combination of the first two solutions; where subscriber packages are defined. However, on top of the packages, the bandwidth is limited per service (subscriberless mode) or per subscriber (anonymous subscriber mode).

Configuring the Capacity Control and Tiered Subscriber Services Solution

In this solution, you add a global controller, limit the global controller bandwidth to 500 kbps, and assign the global controller to the P2P service for the Silver and Gold packages.

- Step 1 Configure the solution as described in Configuring the Tiered Subscriber Services Solution, page 15.
- Step 2 Add a new global controller and set a single value for the maximum bandwidth limit for this global controller.
 - a. In the Policies tab, click Global Policy.
 The Global Bandwidth Settings appear in the right (Rule) pane.
 - b. Above the Upstream interface area, click the add (+) icon.
 The Select addition mode window appears (see Figure 21).

Figure 21 Select Addition Mode Window

×	
Select addition mode	
⊙ Add a new Global Controller	
O Add a Global Controller and map a Rule and a BWC to it	
Next	Cancel

- c. Click the Add a new Global Controller radio button to add a new global controller.
- d. Click Finish.

The Global Controller Settings window appears (see Figure 22).

Figure 22 Global Controller Settings Window

¥ Upstream Global	Controller	Settings
Global Controller S	ettings	
🔇 Global Controller mu	st have a gcN	ameText
Name: The global controller end The global controller car as well as a separate ra Aggregate Global Controller ● The global controller ● The same rate lim O A different rate lim Single Rate Limit (K Global Controller Aggregate Per Link Global Control	forces a L1 ra n enforce an a te limit per SC troller can enforce a t for all time f nit per time fr ops) Rate Limit Unlimited	te limit on traffic that is mapped to it. ggregate rate limit across all SCE links, E link. different rate limit per time frame. rames ame different rate limit per time frame.
○ A different rate lin	nit per time fr	ame
Single Rate Limit (K		
Global Controller	Rate Limit Unlimited	
	oninniced	
		OK Cancel

- **e**. In the Name field, enter P2P GC.
- f. Click the The same rate limit for all time frames radio button.
- **g.** From the Rate limit for the Per Link Global Controller (in Kbps) drop-down list, choose **500 for the maximum bandwidth**.
- h. Click Finish.
- **Step 3** Repeat Step 2 to add an identical global controller for downstream.
- **Step 4** Apply the P2P global controller to the Silver package.
 - a. Click the Silver package, and click the edit (<u>)</u> icon. The Package Settings dialog box appears.
 - In the Package Settings dialog box, click the Subscriber BW Controllers tab. The Subscriber BW Controllers tab appears (see Figure 23).

Figure 23 Subscriber BW Controllers Tab

Jpstream Subscriber relative priority (upstrea	m): 9	~				•	Ŷ	×
Name		CIR (L3	3 PIR (L	.3	Global Controller		AL	
Primary Upstream BWC		0	Unlimite					
Default Upstream BWC		0	Unlimite	ed	Default Global Controller		1	
	o Calls	256	Unlimite	ed	Default Global Controller		9	
Dpstream P2P		256	1024		Default Global Controller		1	
Upstream Browsing	eam):	9 💌	Unlimite	ed	Default Global Controller	•	5	×
Upstream Browsing			Unlimite PIR (L3		Default Global Controller	() AL	-	×
Upstream Browsing Downstream Subscriber relative priority (downstr		9 💌 R (L3	PIR (L3 Unlimited	Glo	bal Controller	() AL	-	×
Upstream Browsing Downstream Subscriber relative priority (downstr		9 💌 R (L3	PIR (L3 Unlimited Unlimited	Glo	bal Controller ult Global Controller	1	-	×
Subscriber relative priority (downstr Name	CIF 0 0 ide256	9 💌 R (L3	PIR (L3 Unlimited Unlimited Unlimited	Glo Defa Defa	bal Controller ult Global Controller ult Global Controller	1 9	-	×
Upstream Browsing Upstream Subscriber relative priority (downstr Name Primary Downstream BWC Default Downstream BWC	CIF 0 0 ide256 256	9 🔽	PIR (L3 Unlimited Unlimited Unlimited 5000	Glo Defa Defa	bal Controller ult Global Controller ult Global Controller ult Global Controller	1 9 1	-	×
Upstream Browsing Downstream Subscriber relative priority (downstr Name	CIF 0 0 ide256	9 🔽	PIR (L3 Unlimited Unlimited Unlimited	Glo Defa Defa	bal Controller ult Global Controller ult Global Controller	1 9	-	×

- c. In the Upstream P2P row, in the Global Controller column, choose P2P GC.
- **d**. Repeat Step **c** for downstream.
- e. Click OK.

Step 5 Repeat Step 4 for the Bronze package.

Traffic Optimization Reports

There are several reports that can be generated to assist in traffic optimization for the local links. Use the Cisco Insight to get the reports.

3 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. © 2015 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore **Europe Headquarters** Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.