Cisco Service Control Solution Guide

Cisco Service Control Product Overview, Release 4.0.x

Revised: May 27, 2013, OL-29091-01

Note This document supports all 4.0.x releases.

1 About this Guide

The *Cisco Service Control Product Overview* provides a solution-oriented overview of the Cisco Service Control platform, its functionality, and components. It describes the common value propositions that you can implement with Cisco Service Control and provides the high-level steps to implement these value propositions.

This document is intended for service provider system administrators or network engineers.

2 Service Control Overview

The complete Cisco Service Control solution is delivered through a combination of purpose-built hardware and specific software and ecosystem components.

The Cisco Service Control Engine (Cisco SCE) platform supports classification, analysis, and control of Internet or IP traffic; all of which it achieves through the use of deep packet inspection (DPI).

The Cisco Service Control solution enables service providers to create profitable new revenue streams while capitalizing on their existing infrastructure. Using Cisco Service Control, service providers can analyze, charge for, and control IP network traffic at multigigabit and 10-gigabit wire line speeds. The solution also provides the tools needed to identify and target high-margin content-based services and enable their delivery.

Deep Packet Inspection

Packet inspection technology inspects traffic as it travels past an inspection point. Whereas standard networking equipment looks only at the packet TCP/IP header information, DPI looks at the applications delivered over these packets as they pass the inspection point. DPI aids service providers in a wide range of applications:

- Allows service providers to classify all IP applications
- Provides subscriber awareness to manage traffic streams based on the subscriber state and policy
- Provides information to perform network usage analysis and reporting
- Allows service providers to implement capacity management and fair use policies which can in turn allow the service provider to perform these actions:
  - Gain visibility into network activities.
  - Optimize network bandwidth and improve network performance.
  - Guarantee a consistent quality level for all subscribers.
  - Identify and mitigate malicious activities.
- Allows service providers to create tiered services and other differentiated services, such as parental control or turbo buttons.

Service Control Value Propositions

You can use DPI to create many value propositions service providers may implement by using the Cisco Service Control solution. This section describes some common value propositions. However, many more possible value propositions exist.

Each of these value propositions is a single use-case scenario for the Cisco Service Control solution. For more information on high-level steps to implement each value proposition, see the "Value Proposition Implementations" section on page 12.

Application Granularity Usage Analysis

You can use the Cisco Service Control solution to understand how the network is used at a level that provides information that is more granular than packet-level statistics or general bandwidth statistics.

The Cisco Service Control solution can provide:

- Per-subscriber or per-application statistics for specific applications that subscribers are using and when they are using them.
- Subscriber demographics such as the percentage of subscribers using over-the-top (OTT) voice or the amount of bandwidth that is being used by high-use subscribers.

The motivation for understanding network use at this level may include:

- Providing a correlation between direct expenses that relate to bandwidth consumption and the application traffic that generates the expenses.
- Correctly sizing and planning the potential expansion of network equipment and pipes by identifying the distribution of bandwidth consumption between applications. For example, characterizing bandwidth distribution as upstream or downstream, in PoP or out of PoP, and on-Net or off-Net.
- Planning of potential blocking or bandwidth throttling of applications.
- Obtaining general-purpose statistics of the application parameters of the applications that run through the network (such as HTTP servers or streaming servers).
- Fixing network problems that require understanding the application distribution of certain application parameters.

To implement this value proposition, see the "Application Granularity Usage Analysis" section on page 13.

Capacity Control

Use the Cisco Service Control solution to manage subscribers and applications such that you implement a fair-use policy for all subscribers and applications. The solution can be used to implement these capacity control scenarios:

- Peer-to-Peer upload bandwidth management—Upstream Peer-to-Peer traffic bandwidth can be managed on a per-session or per-bandwidth basis.
- Time-based control—Policies can be applied for peak and off-peak network use.
- Congestion-based control—During congestion periods, priority can be given to delay sensitive applications.
- Subscriber fairness—Network resources are fairly allocated between subscribers in real time and over long time periods.
- Destination-based control—Different policies can be created for on-net, peering, or transit traffic.

The Fair Usage traffic management scheme:

- Ensures that every subscriber receives a fair share of the bandwidth and that each individual application flow receives a fair share of bandwidth within the allocation to a subscriber
- Provides fairness across different styles of consumption (burst traffic versus constant traffic) by accounting for the delivered experience a subscriber gets over the course of a measurable duration (for example, 1 hour)
- Automatically adapts to subscribers who use high-priority delay-sensitive applications
- Counts and controls volume quotas and bandwidth without per-application differentiation

The Fair Usage traffic management scheme enables service providers to:

- Apply an equitable distribution of network resources
- Improve the quality of experience that the network provides
- Minimize service abuse

To implement this value proposition, see the "Capacity Control" section on page 13.

Quota Management

The Cisco Service Control solution enables you to offer application-based volume-quota products. Application-based quota products normally apply application-based limits on the volume quotas that a subscriber may consume on a per-application basis or over some period of time.

Application-based volume quota products serves two complementary service provider objectives:

- Limiting the use of high bandwidth-consuming applications. Quota management helps avoid the negative effects on the service provider operation.
- Potentially increases revenue by enriching and differentiating the products offered by the service provider.

Several business use-cases that are based on application-quota management exist:

- Implementing Fair-Usage-Policy—Mitigating the use of high bandwidth-consuming applications and, by this, limiting their negative effects on the network operation.
- Offering Rich tiered services—For example, creating service tiers that are based on a monthly application quota use.
- Implementing Advanced billing schemes—Using the SCE to manage and report application quota for billing purposes.

To implement this value proposition, see the "Quota Management" section on page 14.

Application-Based Billing

This value proposition uses the Cisco Service Control solution to create records at an application granularity level that are sent to a collection or mediation system that then feeds a billing system. This is similar to the Quota Management value proposition, where service providers use service control to enable application-based volume quota products or other quota products that use service control to create billing records for these quota products.

It is also possible to use Service Control only for the creation of these records. The records can include data on bandwidth, volume, duration of application sessions, or instances of use of specific application items.

To implement this value proposition, see the "Application-Based Billing" section on page 14.

Content Filtering and Parental Control

When browsing the Internet, subscribers are concerned about the content. There are numerous web sites that contain inappropriate information.

Use the Cisco Service Control solution to:

- Limit access to pre-defined websites
- Limit access to pre-approved applications
- Redirect HTTP requests to a portal page
- Change the policy in real-time

This content filtering is achieved by:

- Using an internal list of URLs to categorize the HTTP request
- Integrating the SCE with a third party database that categorizes URLs (chat, gaming, adult, gambling), after which the SCE acts based on the predefined rules
- Using a Value Added Server (VAS) to perform the classification

To implement this value proposition, see the "Content Filtering and Parental Control" section on page 14.

Tiered Subscriber Services

You can use the Cisco Service Control solution to create tiered subscriber services including turbo buttons, self-provisioning, and other advanced product offerings.

Table 1 lists an example of a possible tiered policy.

Table 1 Tiered Policy

Network Use	Lesser than 2.8 GB	Lesser than 4.2 GB	Lesser than 5.6 GB	Greater than 5.6 GB
E-mail and browsing	256 kbps	256 kbps	Unlimited	Unlimited
Audio and video streaming	48 kbps	64 kbps	128 kbps	Unlimited
Peer-to-Peer	16 kbps	28 kbps	28 kbps	48 kbps

The tiering of services is defined by the quota used for a given period. For example, when a subscriber uses up the quota allocation, the bandwidth allocation is reduced to dial-up speed. The subscriber can either continue at the reduced speed or upgrade the quota level until the end of the quota period (typically one month).

You can design and implement numerous other tiering plans, depending on your needs. DPI within the SCE enables you to identify many different applications and services and to create custom tiers.

To implement this value proposition, see the "Tiered Subscriber Services" section on page 15.

Mitigating Outgoing Spam

Various types of attacks and malicious traffic that originate from the Internet have increased the need for protection. Denial of Service (DoS) and distributed DoS (DDoS) attacks, worms, viruses, malicious HTTP content, and multiple types of intrusions are common.

Cisco SCE platforms can be deployed inline and are stateful and programmable. Using these features the Cisco SCE platform can detect and mitigate the effect of malicious traffic on service providers and their customers.

The Cisco Service Control solution includes service security functionality comprising anomaly detection, outgoing spam and mass-mailing detection, and signature detection. This functionality enables the Cisco SCE platform to address many of the threats that exist in current networks.

The Cisco Service Control solution uses the mass-mailing activity detection approach to detect and mitigate outgoing spam.

This mechanism is based on monitoring Simple Mail Transfer Protocol (SMTP) session rates. It uses the subscriber-awareness of the Cisco SCE platform and can work in subscriber-aware or anonymous subscribers mode. SMTP is a protocol used for sending e-mails; an excess session rate originating from an individual subscriber is usually indicative of a subscriber creating outgoing spam, which is either deliberate or because of a spam zombie infection.

This detection approach provides operators with several possible courses of action that can be implemented based on their business needs:

- Monitor—Inspect the outgoing spam activity detected. This can be performed by using reports that are based on information collected for the detected outgoing spam activity.
- Block—Automatically block outgoing spam activity that is detected by the Cisco SCE platform to avoid threat propagation and adverse effects to the network.
- Notify—Notify subscribers that they are involved in outgoing spam activity by redirecting their web sessions to a captive portal.

To implement this value proposition, see the "Mitigating Outgoing Spam" section on page 15.

Advertising: Behavioral Targeting

Online advertising is a growing segment within networks, and ISPs have a large amount of behavioral data from their subscribers.

The Cisco Service Control solution can enable behavioral targeting based on an analysis of subscriber usage patterns. The Cisco SCE mirrors browsing traffic of a user to profiling servers, or it analyzes user browsing sessions, detects the significant events (ClickStream), and generates Raw Data Records (RDRs). To avoid compromising subscriber privacy, the RDRs can be configured to not include any Personally Identifiable Information (PII). The Cisco Service Control solution also supports advanced Opt In and Opt Out functionality that allows subscribers to protect their privacy by preventing their traffic from being analyzed.

ClickStream detection is a fundamental capability of the solution, because it can detect which specific requests (out of the many HTTP requests generated throughout the subscriber web activity) are triggered by the subscriber. This greatly reduces the number of requests to be analyzed, which is necessary to enable a scalable analysis solution.

To implement this value proposition, see the "Advertising: Behavioral Targeting" section on page 15.

3 Service Control Components

The Cisco Service Control Application for Broadband (Cisco SCA BB) is the Cisco Service Control solution that enables broadband service providers to gain network-traffic visibility, to control the distribution of network resources, and thereby to optimize traffic in accordance with their business strategies. It enables service providers to reduce network costs, improve network performance and customer experience, and create new service offerings and packages.

System Components

The Cisco Service Control solution consists of four main components:

- The Service Control Engine (Cisco SCE) platform—A flexible and powerful, dedicated network-usage DPI monitoring and control element that is purpose-built to analyze, report, and condition network transactions at the application level.

  For more information about the installation and operation of the Cisco SCE platform, see these Cisco SCE platform installation and configuration guides:

  - *Cisco SCE 8000 10GBE Installation and Configuration Guide*
  - *Cisco SCE 8000 GBE Installation and Configuration Guide*
  - *Cisco SCE 2000 Installation and Configuration Guide*
  - *Cisco SCE 1000 2xGBE Installation and Configuration Guide*
- Cisco Service Control Application for Broadband (Cisco SCA BB) Console—A GUI application for creating policies that control and manage network bandwidth usage by protocols, services, applications, and subscribers.

  For more information about the installation and operation of the Cisco SCA BB, see the *Cisco Service Control Application for Broadband User Guide*.

  - Service Control Application (Cisco SCA) Reporter—A software component that processes data stored by the Collection Manager and provides a set of insightful reports from this data. The Cisco SCA Reporter can run as a standalone or as an integrated part of the console.

    For more information about the installation and operation of the Cisco SCA Reporter, see the *Cisco Service Control Application Report User Guide*.
- Cisco Service Control Collection Manager—An implementation of a collection system that receives Raw Data Records (RDRs) from one or more Cisco SCE platform. It collects usage information and statistics, and stores them in a database. The Cisco Service Control Collection Manager also converts subscriber usage information and statistics into simple text-based files for further processing and collection by external systems.

  For more information about the installation and operation of the Cisco Service Control Collection Manager, see the *Cisco Service Control Management Suite Collection Manager User Guide*.
- Cisco Service Control Subscriber Manager—A middleware software component that is used where dynamic binding of subscriber information and policies is required. The Cisco Service Control Subscriber Manager manages subscriber information and provisions it in real time to multiple Cisco SCE platforms. The Cisco Service Control Subscriber Manager can store subscriber policy information internally, and act as a stateful bridge between the authentication, authorization, and accounting (AAA) system (such as RADIUS and DHCP) and the Cisco SCE platforms.

  For more information about the installation and operation of the Cisco Service Control Subscriber Manager, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

  - Cisco Service Control Quota Manager—An optional component of the Cisco Service Control Subscriber Manager. It enables the Cisco Service Control solution providers to manage subscriber quota across subscriber sessions with a high degree of flexibility.

    For more information about the installation and operation of the Cisco Service Control Quota Manager, see the *Cisco Service Control Management Suite Quota Manager User Guide*.

Together, the Cisco SCE platform, the Cisco SCA BB Console, the Cisco Service Control Collection Manager, and the Cisco Service Control Subscriber Manager are designed to support detailed classification, analysis, reporting, and control of IP network traffic. The Cisco Service Control Collection Manager and the Cisco Service Control Subscriber Manager are optional components; not all deployments of the Cisco Service Control solution require them.

Service Control Engine

The Cisco SCE platform, which is the hardware component of the Cisco Service Control solution, is designed to support observation, analysis, and control of Internet or IP traffic. Table 2 summarizes model information for the Cisco SCE 8000 platform.

Table 2 Cisco SCE 8000 Platform Model Information

Model number	Cisco SCE 8000 10 GBE
Link Type	10 Gigabit Ethernet
Number of Ports	2 or 4
Number of Links	1 or 2

Table 3 summarizes model information for the Cisco SCE 2000 platform.

Table 3 Cisco SCE 2000 Platform Model Information

Model number	Cisco SCE 2020 4xGBE
Link Type	Gigabit Ethernet
Number of Ports	4
Number of Links	2

The Cisco SCE platform offers a number of basic implementation options that enables you to tailor the Cisco SCE platform to fit the needs of a particular installation. An understanding of the various issues and options is crucial to designing, deploying, and configuring the topology that best meets the requirements of the individual system.

Implementation Considerations

There are several issues that must be considered to derive an optimum configuration of the topology-related parameters:

- Functionality—Will the system be used solely to monitor traffic flow with only report functionality, or will it be used for traffic flow control with enforcement and report functionalities?
- Number of links—The Cisco SCE may be connected to one or two gigabit Ethernet (GBE) or 10GBE links. This is relevant to both Inline and Receive-Only topologies.
- Links bandwidth—The Cisco SCE must be installed in a location such that the bandwidth of the links does not exceed the bandwidth of the Cisco SCE.
- Redundancy—Should the system be designed to guarantee uninterrupted Cisco SCE functionality? If so, there must be a backup Cisco SCE platform to assume operation in case of failure of the primary device.
- Link continuity—How should the Cisco SCE respond to platform failure related to link continuity? Should traffic flow continue even though the unit is not operating, or be halted until the platform is repaired or replaced?

These issues determine three important aspects of system deployment and configuration:

- The number of Cisco SCE platforms and the method of installation.
- Physical topology of the system—This is the actual physical placement of the Cisco SCE in the system.
- Topology-related configuration parameters—The correct values for each parameter must be ascertained before configuring the system to ensure that the system functions in the desired manner.

Functionality

The Cisco SCE can serve one of two general functions:

- Monitoring and Control—The Cisco SCE monitors and controls traffic flow. Decisions are enforced by the Cisco SCE depending on the results of the monitoring functions of the Cisco SCE and the configuration of the Cisco SCA BB or Mobile solution.

  To perform control functions, the Cisco SCE must be physically installed as an inline installation and the connection mode must be inline.

- Monitoring—The Cisco SCE monitors traffic flow, but cannot control it.

  Either an inline installation or an optical splitter installation may be used. In the latter scenario, connection mode must be receive-only.

Number of Links

The Cisco SCE can be deployed in a single GBE, two GBE, single 10 GBE, or two 10 GBE links. The two-link topology may implement load-sharing and the Cisco SCE in this case is able to process both directions of a bidirectional flow even if they split to both links.

Links Bandwidth

The bandwidth capacity of the Cisco SCE has a finite limit that varies depending on the configuration. When installing the Cisco SCE, you must ensure that the bandwidth capacity of the links that connect to the SCE does not exceed the bandwidth capacity of the Cisco SCE.

Redundancy

When a high degree of reliability is desired, a second Cisco SCE platform should be installed to provide backup capabilities. The combination of two Cisco SCEs guarantees uninterrupted functioning in case of a failure of one of the platforms. The two Cisco SCEs are cascaded so that, although all processing is performed only in the active Cisco SCE, the standby Cisco SCE is constantly updated with all necessary information so that it can instantly take over processing the traffic on the data links, should the active Cisco SCE fail.

If only preservation of the network links is required, and uninterrupted functionality of the Cisco SCE is not required, one Cisco Cisco SCE is sufficient.

Link Continuity

The bypass mechanism of the Cisco SCE allows traffic to continue to flow, if desired, even if the device is not functioning.

Note that when the Cisco SCE is connected to the network through an optical splitter, a failure of the Cisco SCE does not affect the traffic flow, as the traffic continues to flow through the optical splitter.

Cisco SCE 8000 with Dual Cisco SCE 8000-SCM Modules

The Cisco SCE 8000 supports two Cisco SCE 8000-SCM processor modules. The Cisco SCE 8000-SCM modules are installed in slots 1 and 2 of the Cisco SCE 8000 chassis.

The Cisco SCE 8000-SCM in slot 1 performs both processing and management functions. The Cisco SCE 8000-SCM in slot 2 serves only DPI and traffic processing purposes, doubling the performance and capacity of the Cisco SCE 8000. Although the two modules are identical (with the same ports and LEDs), the second Cisco SCM module does not run chassis management or control software.

Cisco SCE Integration in the Mobile Environment Using Gx or Gy Interfaces

The Cisco SCA-BB 3.8.x supports the Gx reference point for policy provisioning as described in Third Generation Partnership Project (3GPP) TS 29.210 and the Ro reference point (Gy interface) for online charging as described in 3GPP TS 32.299.

Gx Interface

The Gx interface is used to connect between the Policy and Charging Rules Function (PCRF) server and the Cisco SCE. Subscriber parameters, both Cisco SCE-specific (for example, package id), and non-Cisco SCE-specific parameters, known as RADIUS vendor specific attributes (VSAs), can be configured to the Cisco SCE through the Gx interface. The subscriber parameter update can be triggered both by Cisco SCE events, such as login and logout, and by PCRF external events.

The Gx interface can also be used as an additional subscriber integration method. When using the Gx interface as a subscriber integration method, the PCRF provides the subscriber name in addition to the subscriber parameters.

Gy Interface

The Cisco SCA BB works with the Gy protocol interface in addition to working with Cisco SCE-propriety protocol for external quota management. The external quota management support is based on the current Quota Manager support.

For more information about the Cisco SCE integration in mobile environment using the Gx or Gy interfaces, see the *Cisco Service Control Mobile Solution Guide*.

Cisco SCA BB Console

The Cisco SCA BB Console is a GUI application to edit and distribute traffic management policies to Cisco SCE devices.

Using the GUI, you control how classification, reporting, and control are performed by editing service configurations and applying them to the Cisco SCE platform.

There are three stages of traffic processing:

- Classification—The Cisco SCA BB analyses traffic flows and determines their type. For example, browsing, e-mail, file sharing, or voice.
- Accounting and reporting—The Cisco SCA BB performs bookkeeping and generates RDRs that let you analyze and monitor the network.
- Control—The Cisco SCA BB limits and prioritizes traffic flows according to their service, subscriber-package, subscriber quota state, and so on.

The Cisco SCA BB Console also includes the following tools:

- Network Navigator—To set up and manage the network connections to the Cisco Service Control components in your network.
- Cisco SCA Reporter—To create charts and tables that graphically represent bandwidth usage in your network based on many different metrics.
- Signature Editor—To create and modify files that can add and modify protocols and protocol signatures in Cisco SCA BB.
- Cisco Service Control Subscriber Manager GUI—To connect to a Cisco Service Control Subscriber Manager and then manage subscribers, assign packages to subscribers, edit subscriber parameters, and manually add subscribers.
- Anonymous Group Manager GUI—To manage anonymous groups in SCEs.

Service Configuration

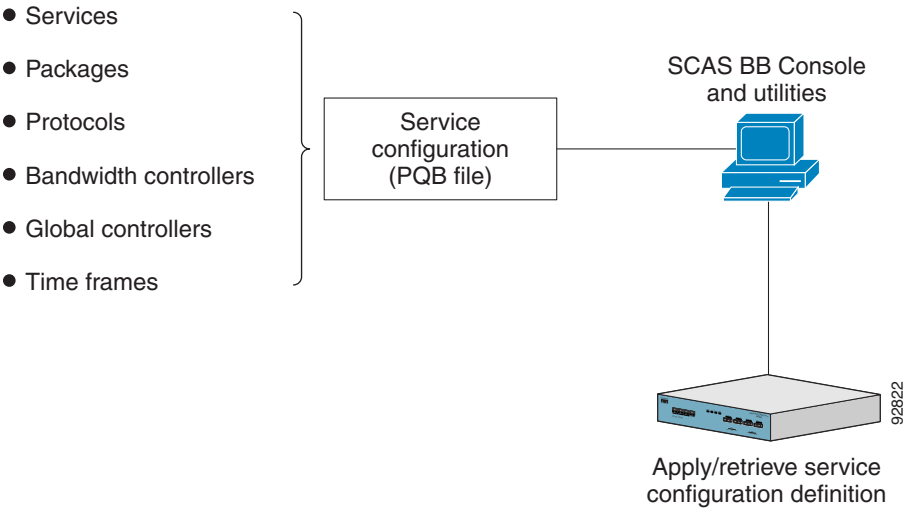
A service configuration defines the way the Cisco SCE platform analyses and controls traffic. In general terms, service configuration defines the following:

- Protocol and service classification
- Packages and policies
- Bandwidth controllers
- Global controllers

The service configuration is contained in a file with a .pqb extension. Service configuration files are commonly referred to as PQB files.

Figure 1 illustrates the service configuration.

Figure 1 Service Configuration



Service configuration is accomplished by using one of these:

- Cisco SCA BB Console
- Cisco SCA BB Service Configuration Utility
- Service Configuration API

Service Configuration Utility

The Cisco SCA BB Service Configuration Utility (servconf) is a command-line utility that you can use to apply PQB configuration files onto Cisco SCE platforms or to retrieve the current configuration from a Cisco SCE platform and save it as a PQB file. The utility configures Cisco SCE platforms with the service configuration defined in a PQB file. You can install and execute it in a Windows or Solaris environment.

Service Configuration API

The Service Configuration API is a set of Java classes that communicate with the Cisco SCE platform and can be used to:

- Program and manage service configurations
- Apply service configurations to the Cisco SCE platforms
- Integrate applications with third-party systems

This allows service providers to automate and simplify management and operational tasks.

The Service Configuration API is documented in the *Cisco SCA BB Service Configuration API Programmer Guide*.

Cisco SCA Reporter

The Cisco SCA Reporter enables you to produce reports based on the traffic analysis performed by the Cisco SCE platform. The information is sent from the Cisco SCE platform to the Cisco Service Control Collection Manager and is stored in a database. The Cisco SCA Reporter can query and retrieve information from the database and present the results in a comprehensive range of reports, including global monitoring, subscriber monitoring, Peer-to-Peer, and traffic discovery statistics reports.

The Cisco SCA Reporter is a valuable tool for understanding the habits and resource consumption of the applications and subscribers that use your network. It can also be used to judge the efficacy of various rules and the possible impact of their implementation on the network.

The Cisco SCA Reporter is available only in a deployment with a Cisco Service Control Collection Manager. You can generate reports by using any of these methods:

- Standalone application
- CLI
- Tool of the Cisco SCA BB Console

The available reports can be customized to:

- Display a variety of chart renderings (for example, stacked-bar or area) or in tabular form.
- Adjust the chart display for various presentation options (for example, 3D).
- Export both tabular and chart reports to files.
- Modify the reports by changing the values assigned to the properties (for example, time boundaries).
- Duplicate, export, and save reports.

You can also generate reports by using the Cisco SCA Reporter CLI without using the GUI.

Cisco Service Control Collection Manager

The Cisco Service Control Collection Manager software package performs these functions:

- Collects the incoming RDR from an Cisco SCE platform.
- Adds an arrival time stamp and the ID of the source Cisco SCE platform to the RDR.

The Cisco Service Control Collection Manager can use either a bundled database or an external database (Oracle, MySQL, or Sybase) to store RDRs supplied by the Cisco SCE platforms of the system. The Cisco Service Control Collection Manager bundled database is the Sybase Adaptive Server Enterprise database, which supports transaction-intensive enterprise applications. The database enables you to store and retrieve information online and can warehouse information as needed.

The Cisco Service Control Collection Manager uses adapters (software modules) to transform RDRs to match the target system requirements and to distribute the RDRs upon request. The Cisco Service Control Collection Manager contains the following adapters:

- Java Database Connectivity (JDBC)
- Comma separated value (CSV)
- Topper/Aggregator (TA)
- Real-time aggregator (RAG)

Some of the adapters send data to the database or write it to CSV files. The structures of the database tables, and the location and structures of the CSV files are described in *Cisco Service Control Application for Broadband Reference Guide*.

When the Cisco Service Control Collection Manager is used in the Cisco Service Control solution, the SCA Reporter queries the Collection Manager database to create charts and graphs of the subscriber network use.

The Cisco Service Control Collection Manager is an optional component. You can create a solution with the Collection Manager, without the Collection Manager, or with a third-party collection manager implementation.

Cisco Service Control Subscriber Manager

The Cisco Service Control Subscriber Manager is a middleware software component that supplies subscriber information for multiple SCE platforms in deployments where dynamic subscriber awareness is required. It does this in one of two ways:

- By pre-storing the subscriber information
- By serving as a stateful bridge between a AAA system or a provisioning system and the SCE platforms

The Cisco SCE platforms use subscriber information to provide subscriber-aware functionality, per-subscriber reporting, and policy enforcement.

To implement a subscriber-aware solution, you must include a Cisco Service Control Subscriber Manager. You can install the Cisco Service Control Subscriber Manager, or you can create your own subscriber management module and use the Cisco SCE Subscriber API to integrate with the Cisco SCE platform. For further information, see the *Cisco SCMS SCE Subscriber API Programmer Guide*.

Some Cisco Service Control solutions can also operate without subscriber awareness:

- Subscriber-less—Control and link-level analysis functions are provided at a global device resolution. For example, monitoring and managing the total bandwidth consumed by Peer-to-Peer traffic over the link.
- Anonymous subscriber—The system dynamically creates *anonymous* subscribers per IP address. User-defined IP address ranges may then be used to differentiate between anonymous subscriber policies. Use this mode when you do not require subscriber-differentiated control or subscriber-level quota tracking, when analysis on an IP level is sufficient, or when offline IP address/subscriber binding can be performed.
- Static subscriber awareness—Subscriber awareness is required, but allocation of network IDs (mainly IP addresses) to subscribers is static. In this mode, traffic to and from defined subscribers is controlled as a group. For example, you can define all traffic from and to a particular network subnet (used by multiple subscribers concurrently) as a (virtual) *subscriber* and controlled or viewed as a group.

In these three modes, the SCE platform handles all subscriber-related functionality without a Subscriber Manager.

Managing Subscribers

The Cisco Service Control Subscriber Manager addresses the following issues in allowing dynamic subscriber awareness:

- Mapping—The Cisco SCE platform encounters flows with network IDs (IP addresses) that change dynamically, and it requires dynamic mapping between those network IDs and the subscriber IDs. The SM database contains the network IDs that map to the subscriber IDs. This is the main functionality of the SM.
- Policy—The Cisco Service Control Subscriber Manager serves as a repository of policy information for each subscriber. The policy information may be preconfigured to the Subscriber Manager, or dynamically provisioned when the mapping information is provided.
- Capacity—The Cisco SCE platform or platforms may need to handle (over time) more subscribers than they can concurrently hold. In this case, the Subscriber Manager serves as an external repository for subscriber information, while only the online or active subscribers are introduced to the SCE platform.
- Location—The Cisco Service Control Subscriber Manager supports the functionality of sending subscriber information only to the relevant Cisco SCE platforms, in case such functionality is required. This is implemented by using the domains mechanism or Pull mode.

The Cisco Service Control Subscriber Manager uses a relational database optimized for high performance and with a background persistency scheme. The In-Memory Database efficiently stores and retrieves subscriber records.

The Cisco Service Control Subscriber Manager database can function in one of two ways:

- As the only source for subscriber information when the Cisco Service Control Subscriber Manager works in standalone mode
- As a subscriber information cache when the Cisco Service Control Subscriber Manager serves as a bridge between a group of Cisco SCE devices and the customer AAA and operations support systems (OSS).

4 Value Proposition Implementations

This chapter provides an overview of how to implement the value propositions that are offered by the Cisco Service Control solution within your network. Each implementation points to the relevant documentation on how to install additional components (if required), how to configure the system, and how to monitor the system.

Prerequisites

To implement any of the value propositions, it is necessary to install these Service Control components:

- Service Control Engine, page 7
- Cisco SCA BB Console, page 9
- Cisco Service Control Collection Manager, page 11

Note Although the Cisco Service Control Collection Manager is an optional component, implementing Cisco Service Control Collection Manager can bring in value propositions.

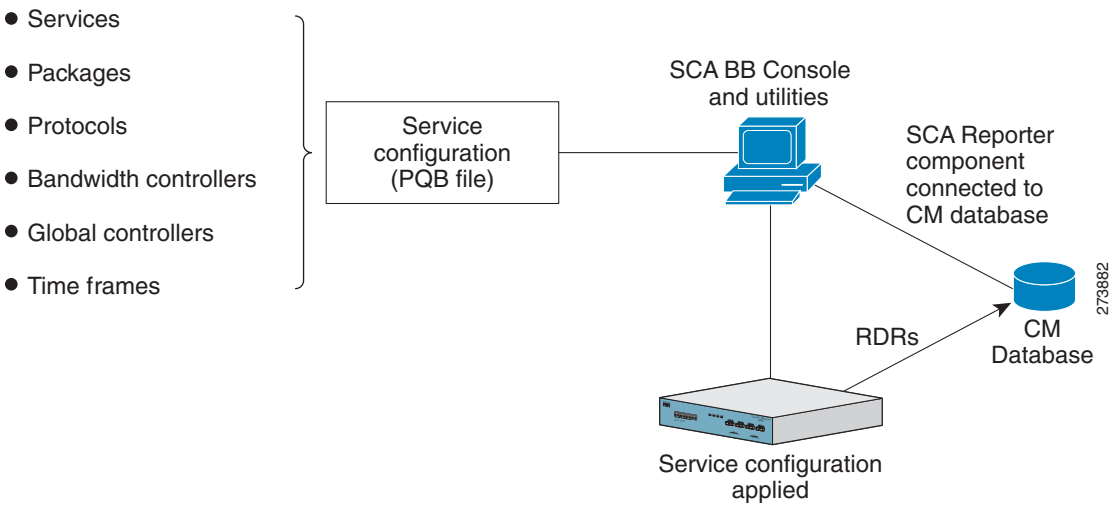
The system should be set up such that:

- Cisco SCA BB Console is connected to the Cisco SCE.
- Cisco SCE is configured with a PQB configuration and is processing traffic and sending RDRs to the Cisco Service Control Collection Manager.
- Cisco SCA Reporter is connected to the database of the Cisco Service Control Collection Manager.

For further information about installing and setting up your system, see *Cisco Service Control Product Installation Guide*.

Figure 2 shows the topology of the solution when it is installed and set up.

Figure 2 Service Control Solution Set up



Application Granularity Usage Analysis

For a description of this value proposition, see the "Application Granularity Usage Analysis" section on page 3.

The main functionality for this value proposition is contained in the Cisco SCA Reporter. The Cisco SCA Reporter is available as a component of the Cisco SCA BB Console or it can be installed as a standalone application.

For more information on using the Cisco SCA Reporter to create reports, see the *Cisco Service Control Usage Analysis and Reporting Solution Guide*. The reports used highlight the capabilities of the Cisco SCA Reporter to identify application, bandwidth, and subscriber use.

Capacity Control

For a description of this value proposition, see the "Capacity Control" section on page 3.

The capacity control value proposition requires only the Cisco SCE and the Cisco SCA BB Console and can be provisioned in two ways:

- Capacity control of the local links of the Cisco SCE—For further information on configuring the system in this manner, see the "Managing Bandwidth" section in the "Using the Service Configuration Editor: Traffic Control" chapter of the *Cisco Service Control Application for Broadband User Guide*.
- Capacity control of the remote CMTS links in a cable environment—For more details on configuring the system in the manner, see the "Configuring the Solution" section of the *Cisco Service Control for Managing Remote Cable MSO Links Solution Guide*.

Quota Management

For a description of this value proposition, see the "Quota Management" section on page 4. You can implement this value proposition with the Cisco SCE API or with the Quota Manager component of the Cisco Service Control Subscriber Manager. The following implementation uses the Quota Manager component:

1. To install the Cisco Service Control Subscriber Manager, see the Installing and Upgrading chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.
2. To configure the Cisco Service Control Subscriber Manager and the Cisco SCA BB to use the Quota Manager for quota management, perform the configuration described in the Configuring the Quota Manager chapter of the *Cisco Service Control Management Suite Quota Manager User Guide*.

The *Cisco Service Control Management Suite Quota Manager User Guide* also contains a number of scenarios in which the Quota Manager helps when initially deploying a quota management system.

To implement quota management that uses the SCE internal quota functionality with the Cisco SCA BB, see the "Managing Quotas" section in the "Using the Service Configuration Editor: Traffic Control" chapter of the *Cisco Service Control Application for Broadband User Guide*.

Application-Based Billing

For a description of this value proposition, see the "Application-Based Billing" section on page 4.

A solution that provides application-based billing requires a billing system that is connected to the Cisco Service Control solution:

1. Integrate a billing system with the Cisco Service Control Collection Manager database.
2. Retrieve the Subscriber Usage RDRs from the TA adapter CSV files. The format of the CSV files is described in the "CSV File Formats" chapter of *Cisco Service Control Application for Broadband Reference Guide*.

For details on managing and using RDRs, see the:

- "Managing RDR Settings" section in the "Using the Service Configuration Editor: Traffic Accounting and Reporting" chapter of the *Cisco Service Control Application for Broadband User Guide*.
- "Raw Data Records: Formats and Field Contents" chapter of the *Cisco Service Control Application for Broadband Reference Guide*.

Content Filtering and Parental Control

For a description of this value proposition, see the "Content Filtering and Parental Control" section on page 4.

You can implement the content filtering and parental control value proposition in three ways:

- Use the URL flavor mechanism of the Cisco SCE—The solution is automatically configured to use the URL flavor mechanism, which uses an internal database of URLs, and no further action needs to be taken.
- Integrate the Cisco SCA BB Console and an external content filtering or parental control server. An example configuration is provided in the "Managing Content Filtering" section in the "Using the Service Configuration Editor: Traffic Classification" chapter of *Cisco Service Control Application for Broadband User Guide*.
- Use the Cisco SCE blacklisting mechanism. The configuration is described in the *Cisco Service Control URL Blacklisting Solution Guide*.

Tiered Subscriber Services

For a description of this value proposition, see the "Tiered Subscriber Services" section on page 4.

This value proposition requires the Cisco Service Control Subscriber Manager module.

1. To install the SM, see the Installing and Upgrading chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.
2. To create tiered subscriber services, see the "Example: Creating Tiered Subscriber Services" section in the "Using the Service Configuration Editor: Traffic Control" chapter of the *Cisco Service Control Application for Broadband User Guide*.

Mitigating Outgoing Spam

For a description of this value proposition, see the "Mitigating Outgoing Spam" section on page 5.

To mitigate outgoing spam, it is first necessary to determine that you have an outgoing spam problem. After you identify the problem, you can use the Cisco SCE and the Cisco SCA BB Console to mitigate the outgoing spam.

1. To monitor mass-mailing activity, you should create a *Top Subscribers by Sessions* report, which can be used to identify the IDs of subscribers most likely to be involved in mass-mailing activity. See *Cisco Service Control Application Reporter User Guide*.
2. To mitigate outgoing spam, perform the configuration described in the "Mass-Mailing Based Threats" chapter of *Cisco Service Control Service Security: Outgoing Spam Mitigation Solution Guide*.
3. After configuring the system to mitigate outgoing spam, you can create a second Top Subscribers by Sessions report, which indicates whether the mitigation actions were successful.

Advertising: Behavioral Targeting

For a description of this value proposition, see the "Advertising: Behavioral Targeting" section on page 5.

Cisco SCE and the Cisco SCA BB Console implement targeting advertising based on the behavior of subscribers.

Note To implement behavioral advertising, you must also integrate the system with an advertising vendor.

- To implement behavioral advertising that is based on traffic mirroring, perform the configuration described in *Cisco Service Control Online Advertising Solution Guide: Behavioral Profile Creation Using Traffic Mirroring*.
- To implement behavioral advertising that is based on RDR records, perform the configuration described in the *Cisco Service Control Online Advertising Solution Guide: Behavioral Profile Creation Using RDRs*.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, 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.

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**.

OL-29091-01