Cisco Service Control Solution Guide

Cisco Service Control Product Overview

Revised: January, 2009, OL-18875-01

1 About this Guide

This *Cisco Service Control Product Overview* is a solution-oriented overview of the Cisco Service Control platform, its functionality, and components. It describes 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 Service Control Engine (SCE) platform supports classification, analysis, and control of Internet/IP traffic; all of which it achieves through the use of deep packet inspection (DPI).

This Service Control solution enables service providers to create profitable new revenue streams while capitalizing on their existing infrastructure. With the power of 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 enables the following:

- Allows service providers to classify all IP applications
- Provides subscriber awareness to manage traffic streams based on an individual's 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 do the following:
  - 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 that may be implemented by service providers 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. The high-level steps to implement each value proposition are provided in the Value Proposition Implementations chapter.

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 to provide information about the specific applications that subscribers are using and when they are using them.
- Subscriber demographics such as showing the percentage of subscribers that are using over-the-top (OTT) voice or how much bandwidth 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 versus downstream, in PoP versus out of PoP, and on-Net versus 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 12.

Capacity Control

You can use the Cisco Service Control Solution to manage subscribers and applications such that high-bandwidth users can be limited to enable the implementation of a fair-use policy for all subscribers and applications. The solution can be used to implement the following capacity control scenarios:

- Peer to Peer (P2P) upload bandwidth management—Upstream P2P traffic bandwidth can be managed on a per session or on a 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 can be fairly allocated between subscriber in real-time and over long time periods.
- Destination-based control—Different policies can be created for on-net, peering, or transit traffic.

The Cisco Service Control solution includes the FairUsage traffic management scheme to facilitate the above capacity control scenarios. The FairUsage 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

The FairUsage 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 that engage in high-priority delay-sensitive applications
- Counts and controls volume quotas and bandwidth without per application differentiation

To implement this value proposition, see the “Capacity Control” section on page 12.

Quota Management

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 can serve two complementary service provider objectives:

- Limiting the use of high bandwidth-consuming applications. Quota management can help to avoid the negative effects on a service provider's operation.

- Potentially increasing 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.
- Rich tiered services offering—For example, creating service tiers that are based on a monthly application quota use.
- Advanced billing schemes—Using the SCE to manage and report application quota for billing purposes.

The Cisco Service Control solution enables you to offer application-based volume-quota products. To implement this value proposition, see the “Quota Management” section on page 13.

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 13.

Content Filtering and Parental Control

Many subscribers are concerned with the content that appears on their computers when a user browses the Internet. This is especially important, but not limited, to subscribers with children for whom there are a large number of sites and types of content that are unsuitable.

You can use the Cisco Service Control solution to control applications and content:

- Limiting access to pre-defined web-sites
- Limiting access to pre-approved applications
- Redirecting HTTP requests to a portal page
- Changing the policy in real-time

This content filtering can be executed in a number of ways:

- Using an internal list of URLs to categorize the HTTP request
- Integrating the SCE with a 3rd party database that categorizes URLs (chat, gaming, adult, gambling) after which the SCE acts based upon 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 13.

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.

An example of a possible tiered policy is shown in the following table.

Network Use	Less than 2.8 GB	Less than 4.2 GB	Less than 5.6 GB	Greater than 5.6 GB
Email and browsing	256 kbps	256 kbps	Unlimited	Unlimited
Audio and video streaming	48 kbps	64 kbps	128 kbps	Unlimited
P2P	16 kbps	28 kbps	28 kbps	48 kbps

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

Numerous other tiering plans can be designed and implemented according to 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 13.

Mitigating Outgoing Spam

The need for protection from various types of attacks and malicious traffic that originate from the Internet has gained focus. Denial of Service (DoS) and Distributed DoS (DDoS) attacks, worms, viruses, malicious HTTP content, and multiple types of intrusions are common.

SCE platforms are deployed inline and are stateful and programmable. These features position the SCE platform to 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 allows the 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 SCE platform's subscriber-awareness and can work in subscriber-aware or anonymous subscribers mode. SMTP is a protocol used for sending email; an excess rate of such sessions originating from an individual subscriber is usually indicative of a subscriber creating outgoing spam, who is either deliberately sending spam or is infected by a spam zombie.

This detection approach provides operators with several possible courses of action to be implemented based on their business needs.

- Monitor—Inspect the outgoing spam activity detected by this method. This can be performed using reports that are based on information collected for outgoing spam activity that is detected.
- Block—Automatically block outgoing spam activity that is detected by the SCE platform to avoid threat propagation and adverse effects to the network.
- Notify—Notify subscribers that they are detected as being 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 14.

Advertising: Behavioral Targeting

Online advertising is a growing segment within networks, and ISPs have a large amount of behavioral data from their subscribers. The ability of ISPs to translate their knowledge into a profit-generating share of the online advertising market is described in this section.

The Cisco Service Control solution can enable behavioral targeting based on an analysis of subscriber usage patterns. The SCE mirrors a user's browsing traffic to profiling servers, or it analyzes user browsing sessions, detects the significant events (ClickStream), and generates RDRs. To avoid compromising subscriber privacy, the RDRs can be configured not to 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, as it can detect which specific requests (out of the enormous number of 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 14.

3 Service Control Components

The Cisco Service Control Application for Broadband (SCA BB) is the Cisco Service Control solution that allows 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 (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 SCE platform, see the Cisco SCE Platform Installation and Configuration Guides.

  - *Cisco SCE8000 Installation and Configuration Guide*
  - *Cisco SCE 2000 4xGBE Installation and Configuration Guide*
  - *Cisco SCE 1000 2xGBE Installation and Configuration Guide*

- The Service Control Application for Broadband (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 SCA BB, see the *Cisco Service Control Application for Broadband User Guide*.

  - The Service Control Application (SCA) Reporter—A software component that processes data stored by the collection manager and provides a set of insightful reports from this data. The 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 SCA Reporter, see the *Cisco Service Control Application Report User Guide*.

- The Service Control Management Suite (SCMS) Collection Manager—An implementation of a collection system that receives Raw Data Records (RDRs) from one or more SCE platforms. It collects usage information and statistics, and stores them in a database. The 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 Collection Manager, see the *Cisco Service Control Management Suite Collection Manager User Guide*.

- The Service Control Management Suite (SCMS) Subscriber Manager—A middleware software component that is used where dynamic binding of subscriber information and policies is required. The SM manages subscriber information and provisions it in real time to multiple SCE platforms. The Subscriber Manager can store subscriber policy information internally, and act as a stateful bridge between the AAA system (such as RADIUS and DHCP) and the SCE platforms.

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

  - The Quota Manager is an optional component of the Subscriber Manager. It enables 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 Quota Manager, see the *Cisco Quota Manager Solution Guide*.

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

Service Control Engine

The Service Control Engine (SCE) platform, which is the hardware component of the Cisco Service Control solution, is designed to support observation, analysis, and control of Internet/IP traffic. The following table summarizes model information for the Cisco SCE8000 platform.

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

The following table summarizes model information for the Cisco SCE 2000 platform.

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 permit the user to tailor the 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 in order to arrive at the optimum configuration of the topology-related parameters:

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

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

- How many SCE platforms are needed and how will they be installed?
- Physical topology of the system—The actual physical placement of the SCE in the system.
- Topology-related configuration parameters—The correct values for each parameter must be ascertained before configuring the system to make sure that the system will function in the desired manner.

Functionality

The SCE can serve one of two general functions:

- Monitoring and Control—The SCE monitors and controls traffic flow. Decisions are enforced by the SCE depending on the results of the monitoring functions of the SCE and the configuration of the Service Control Application for Broadband or Mobile solution.

  In order to perform control functions, the SCE must be physically installed as an inline installation and the connection mode must be inline.
- Monitoring only—The SCE monitors traffic flow, but cannot control it.

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

Number of Links

The SCE can be deployed in a single gigabit Ethernet (GBE), two GBE, single 10 GBE, or two 10 GBE links. The 2-link topology may implement load-sharing and the 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 SCE has a finite limit that varies depending on the configuration. When installing the SCE, you must ensure that the bandwidth capacity of the links that connect to the SCE do not exceed the bandwidth capacity of the SCE.

Redundancy

When a high degree of reliability is desired, a second SCE platform should be installed to provide backup operation capabilities. The combination of two SCEs guarantees uninterrupted functioning in case of a failure of one of the platforms. The two SCEs are cascaded so that, although all processing is performed only in the active SCE, the standby 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 SCE fail.

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

Link Continuity

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

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

SCA BB Console

The SCA BB Console is a GUI application that you can use to edit and distribute traffic management policies to the SCE.

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

There are three stages of traffic processing:

- Classification—SCA BB analyses traffic flows and determines their type (for example, browsing, email, file sharing, or voice).
- Accounting and reporting—SCA BB performs bookkeeping and generates Raw Data Records (RDRs) that let you analyze and monitor the network.
- Control—SCA BB limits and prioritizes traffic flows according to their service, subscriber-package, subscriber quota state, and so on.

The SCA BB Console also includes the following tools:

- Network Navigator—To set up and manage the network connections to the Service Control components in your network.
- 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 SCA BB.
- Subscriber Manager GUI—To connect to a Subscriber Manager and then manage subscribers, assign packages to subscribers, edit subscriber parameters, and manually add subscribers.

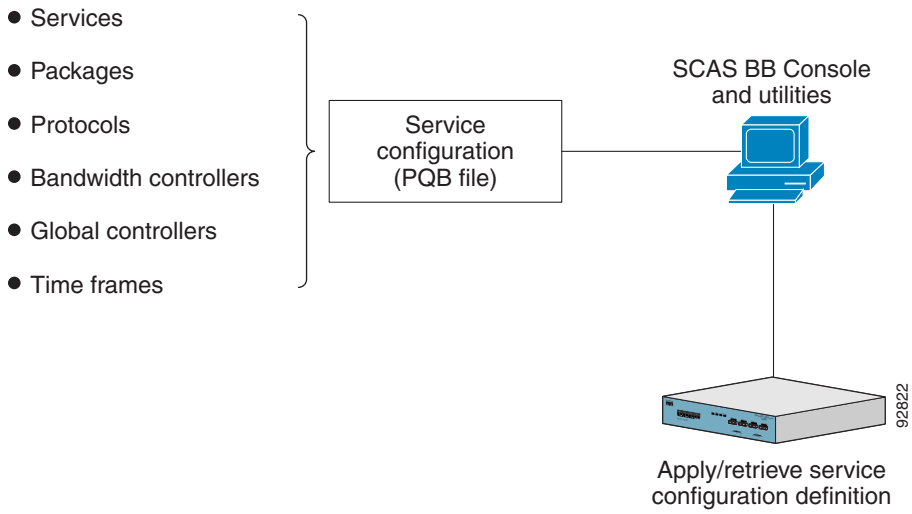
Service Configuration

A service configuration defines the way the 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 Service Configuration



Service configuration is accomplished using one of the following:

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

Service Configuration Utility

The SCA BB Service Configuration Utility (**servconf**) is a command-line utility that you can use to apply PQB configuration files onto SCE platforms or to retrieve the current configuration from an SCE platform and save it as a PQB file. The utility configures 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 SCE platform and can be used to:

- Program and manage service configurations
- Apply service configurations to the 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*.

SCA Reporter

The Cisco Service Control Application Reporter (SCA Reporter) is the Cisco Service Control Application tool that allows you to produce reports based on the traffic analysis performed by the Service Control Engine (SCE) platform. The information is sent from the SCE platform to the Collection Manager and is stored in a database. The 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, P2P, and traffic discovery statistics reports.

The 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 SCA Reporter is available only in a deployment with a Collection Manager. You can generate reports using any of the following methods:

- Standalone application
- Command-line interface (CLI)
- Tool of the SCA BB Console

The available reports can be displayed in a variety of chart renderings (for example, stacked-bar or area) or in tabular form. You can adjust the chart display for various presentation options (for example, 3D). You can export both tabular and chart reports to files. You can also modify the reports by changing the values assigned to the properties (for example, time boundaries). You can duplicate, export, and save reports.

You can also generate reports using the SCA Reporter Command-Line Interface (CLI) without using the GUI.

Collection Manager

The Collection Manager software package:

- Collects the incoming raw data records (RDR) from an SCE platform.
- Adds an arrival timestamp and the ID of the source SCE platform to the RDR.

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

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

- JDBC adapter
- Comma separated value (CSV) adapter
- Topper/Aggregator (TA) adapter
- Real-time aggregating (RAG) adapter

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 these CSV files are described in the *Cisco Service Control Application for Broadband Reference Guide*.

When the 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 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.

Subscriber Manager

The Subscriber Manager is a middleware software component that supplies subscriber information for multiple Service Control Engine (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 an Authentication, Authorization, and Accounting (AAA) system or a provisioning system and the SCE platforms

The 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 subscriber manager. You can install the Cisco SCMS Subscriber Manager, or you can create your own subscriber management module and use the SCE Subscriber API to integrate with the 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 P2P 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 subscribers 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 from and to defined subscribers can be 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 a Subscriber Manager module is not required.

Managing Subscribers

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

- Mapping—The 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 Subscriber Manager database contains the network IDs that map to the subscriber IDs. This is the main functionality of the Subscriber Manager.
- Policy—The 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 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 Subscriber Manager supports the functionality of sending subscriber information only to the relevant SCE platforms, in case such functionality is required. This is implemented using the domains mechanism or Pull mode.

The Subscriber Manager uses a commercial relational database from TimesTen, optimized for high performance and with a background persistency scheme. The In-Memory Database efficiently stores and retrieves subscriber records.

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

- As the only source for subscriber information when the Subscriber Manager works in standalone mode
- As a subscriber information cache when the Subscriber Manager serves as a bridge between a group of SCE devices and the customer Authentication, Authorization, and Accounting (AAA) and Operational 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 the following Service Control components:

- Service Control Engine, page 7
- SCA BB Console, page 8
- Collection Manager, page 10

Note Although the Collection Manager is an optional component, to implement any of the following value propositions requires the Collection Manager.

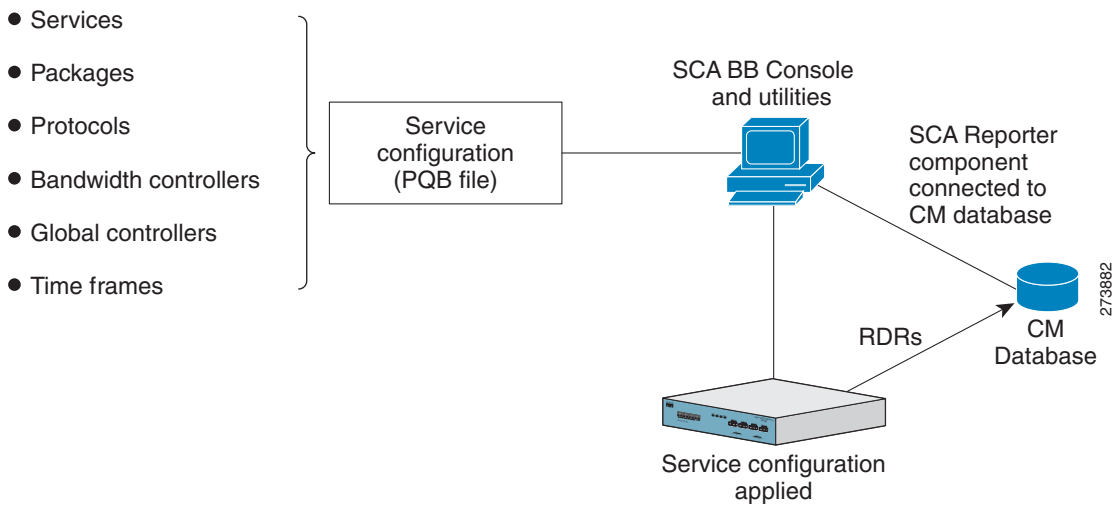
The system should be set up such that:

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

For further information about installing and setting up your system, see the *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 Setup



Application Granularity Usage Analysis

For a description of this value proposition, see the "Application Granularity Usage Analysis" section on page 2.

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

To start using the SCA Reporter to create reports, see the *Cisco Service Control Usage Analysis and Reporting Solution Guide*, which provides an introduction to using the SCA Reporter and a description of a number of the most commonly used reports, how to create them, and sample outputs from these reports. The reports used highlight the capabilities of the 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 SCE and the SCA BB Console and can be provisioned in two ways:

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

Quota Management

For a description of this value proposition, see the "Quota Management" section on page 3. You can implement this value proposition with the SCE API or with the Quota Manager component of the Subscriber Manager. The following implementation uses the Quota Manager component:

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

The *Cisco Quota Manager Solution Guide* also contains a number of quota manager use-cases to help when initially deploying a quota management system.

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

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 Collection Manager database.
2. Retrieve the Subscriber Usage Raw Data Records (RDRs) from the topper/aggregator adapter CSV files. The format of the CSV files is described in the *Cisco Service Control Application for Broadband Reference Guide*, the "CSV File Formats" chapter.

For further information about managing and using RDRs see the following guides:

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

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 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 SCA BB Console and an external content filtering or parental control server. An example configuration is provided in the *Cisco Service Control Application for Broadband User Guide*, the "Using the Service Configuration Editor: Traffic Classification" chapter, the "Managing Content Filtering" section.
- Use the 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 SM module.

1. To install the SM, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*, the Installing and Upgrading chapter.

2. To create tiered subscriber services, see the *Cisco Service Control Application for Broadband User Guide*, the "Using the Service Configuration Editor: Traffic Control" chapter, the "Example: Creating Tiered Subscriber Services" section.

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 SCE and the 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 the *Cisco Service Control Application Reporter User Guide*.
2. To mitigate outgoing spam, perform the configuration described in the *Cisco Service Control Service Security: Outgoing Spam Mitigation Solution Guide*, the "Mass-Mailing Based Threats" chapter.
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.

Targeting advertising based on the behavior of subscribers can be implemented using the SCE and the SCA BB Console.

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 the *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*.

5 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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-18875-01