CHAPTER 1

Cisco Service Control Overview

Revised: February 25, 2015

Introduction

This chapter provides a general overview of the Cisco Service Control solution. It introduces the Cisco service control concept and capabilities.

It also briefly describes the hardware capabilities of the service control engine (Cisco SCE) platform and the Cisco specific applications that together compose the complete Cisco service control solution.

- Cisco Service Control Solution, page 1-2
- Cisco Service Control Capabilities, page 1-3
- Cisco SCE Platform Description, page 1-4
- Management and Collection, page 1-6
- IPv6 Support, page 1-8

Cisco Service Control Solution

The Cisco service control solution is delivered through a combination of hardware and specific software solutions that address various operational and business-related challenges. Service providers can use the Cisco SCE platform to support classification, analysis, and control of Internet and IP traffic.

Service control enables service providers to:

- Capitalize on existing infrastructure.
- Analyze, charge for, and control IP network traffic at multigigabit wire line speeds.
- Identify and target high-margin content-based services and enable their delivery.

As access and bandwidth have become commodities where prices continually fall and profits disappear, service providers have realized that they must offer value-added services to derive more revenue from the traffic and services running on their networks.

Cisco service control solutions allow the service provider to capture profits from IP services through detailed monitoring, precise, real-time control, and awareness of applications as they are delivered.

Service Control for Broadband Service Providers

Service providers of any access technology (DSL, cable, mobile, and so on) targeting residential and business consumers must find new ways to get maximum leverage from their existing infrastructure, while differentiating their offerings with enhanced IP services.

The Cisco service control application for broadband adds a layer of service intelligence and control to existing networks that can:

- Report and analyze network traffic at subscriber and aggregate level for capacity planning
- Provide customer-intuitive tiered application services and guarantee application service level agreements (SLAs)
- Implement different service levels for different types of customers, content, or applications
- Identify network abusers who are violating the acceptable use policy (AUP)
- Identify and manage peer-to-peer traffic, NNTP (news) traffic, and spam abusers
- Enforce the AUP
- Integrate Service Control solutions easily with existing network elements and business support systems (BSS) and operational support systems (OSS)

Cisco Service Control Capabilities

The core of the Cisco service control solution is the network hardware device: the Service control engine (Cisco SCE). The core capabilities of the Cisco SCE platform, which support a wide range of applications for delivering service control solutions, include:

- Subscriber and application awareness—Application-level drilling into IP traffic for real-time understanding and controlling of usage and content at the granularity of a specific subscriber.
  - Subscriber awareness—The ability to map between IP flows and a specific subscriber to maintain the state of each subscriber transmitting traffic through the Cisco SCE platform and to enforce the appropriate policy on this subscriber's traffic.

    Subscriber awareness is achieved either through dedicated integrations with subscriber management repositories, such as a DHCP or a RADIUS server, or through sniffing of RADIUS or DHCP traffic.
  - Application awareness—The ability to understand and analyze traffic up to the application protocol layer (Layer 7).

    For application protocols implemented using bundled flows (such as FTP, which is implemented using Control and Data flows), the Cisco SCE platform understands the bundling connection between the flows and treats them accordingly.
- Application-layer, stateful, real-time traffic control—The ability to perform advanced control functions, including granular bandwidth (BW) metering and shaping, quota management, and redirection, using application-layer, stateful, real-time traffic transaction processing. This requires highly adaptive protocol and application-level intelligence.
- Programmability—The ability to quickly add new protocols and adapt to new services and applications in the service provider environment. Programmability is achieved using the Cisco Service Modeling Language (SML).

  Programmability allows new services to be deployed quickly and provides an easy upgrade path for network, application, or service growth.
- Robust and flexible back-office integration—The ability to integrate with existing third-party systems at the service provider, including provisioning systems, subscriber repositories, billing systems, and OSS systems. The Cisco SCE provides a set of open and well-documented APIs that allows a quick integration process.
- Scalable high-performance service engines—The ability to perform all of these operations at wire speed.

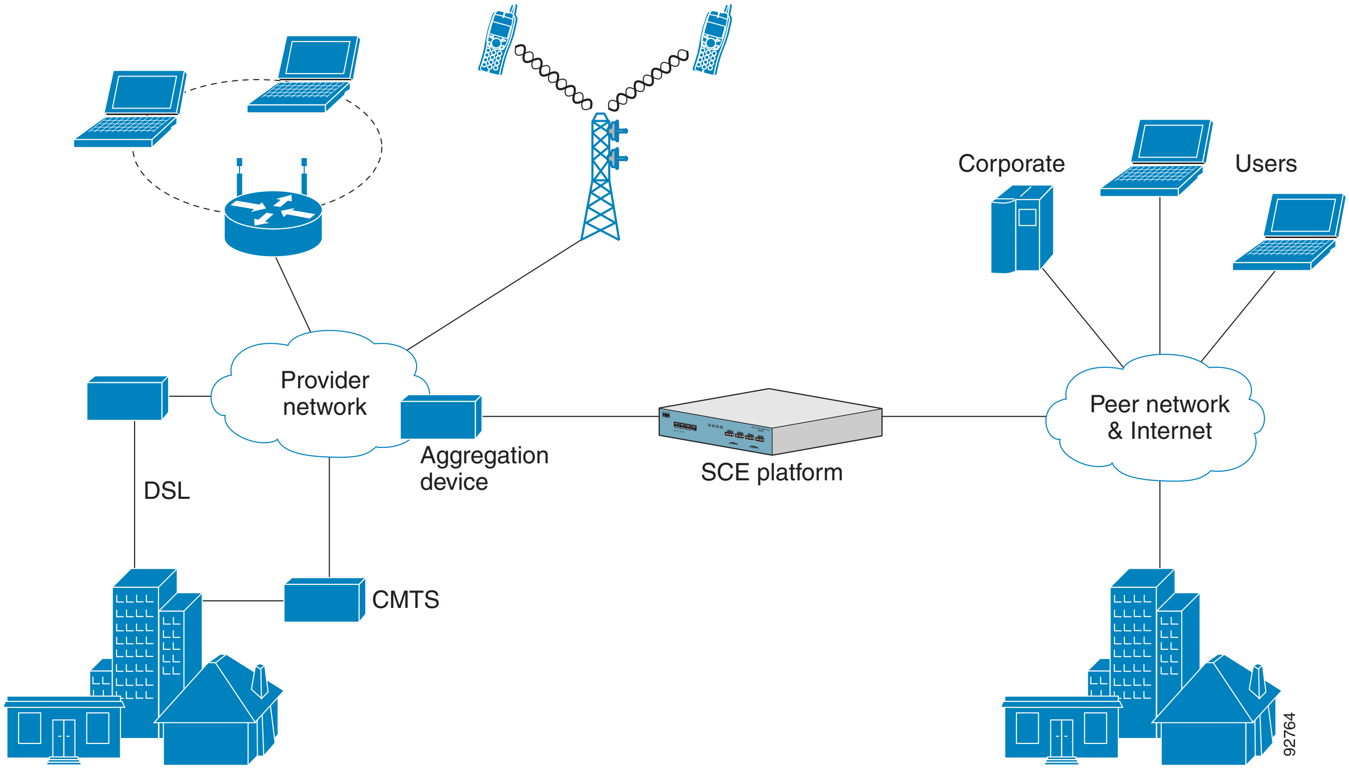
Cisco SCE Platform Description

The Cisco SCE family of programmable network devices performs application-layer stateful-flow inspection of IP traffic, and controls the traffic based on configurable rules. The Cisco SCE platform is a network device that uses ASIC components and reduced instruction set computer (RISC) processors to exceed beyond packet counting and expand into the contents of network traffic. Providing programmable, stateful inspection of bidirectional traffic flows, and mapping these flows with user ownership, Cisco SCE platforms provide real-time classification of network use. The classification provides the basis of the Cisco SCE platform advanced traffic-control and bandwidth-policing functionality. Where most bandwidth control functionality ends, the Cisco SCE platform provides further control and shaping options, including:

- Layer 7 stateful wire-speed packet inspection and classification
- Robust support for more than 600 protocols and applications, including:
  - General—HTTP, HTTPS, FTP, Telnet, Network News Transfer Protocol (NNTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAP), Wireless Application Protocol (WAP), and others
  - Peer-to-Peer (P2P) file sharing—FastTrack-KazaA, Gnutella, BitTorrent, Winny, Hotline, eDonkey, DirectConnect, Piolet, and others
  - P2P VoIP—Skype, Skinny, DingoTel, and others
  - Streaming and Multimedia—Real Time Streaming Protocol (RTSP), Session Initiation Protocol (SIP), HTTP streaming, Real Time Protocol (RTP) and Real Time Control Protocol (RTCP), and others
- Programmable system core for flexible reporting and bandwidth control
- Transparent network and BSS and OSS integration into existing networks
- Subscriber awareness that relates traffic and usage to specific customers

Figure 1-1 illustrates a common deployment of a Cisco SCE platform in a network.

Figure 1-1 Cisco SCE Platform in the Network



Bandwidth Management of P2P Traffic

The Cisco SCE uses unique signatures to identify the networking flows of P2P, IM, and other applications. While defining packages to subscribers, you can create rules for different types of applications such as P2P, and IM and if required, associate these rules to separate Bandwidth Controls (BWCs). With BWC enforcement, you can limit the networking flows for all types of applications. There are three types of rules in the Cisco SCE which can be used for bandwidth enforcement at different levels.

- P2P based BWC

If the Cisco SCE is configured to enforce BWC based on peer-to-peer traffic, it detects the application based on its signature. Cisco SCE then includes the amount of network flows of P2P traffic and calculates the bandwidth accordingly. The consumed bandwidth is the sum of P2P data and the control traffic. Bandwidth limitation takes place as per the enforcement configured in the BWC.

- Default Service BWC

When an application is configured with discrete BWC, the Cisco SCE does not relate the amount of networking flows of the application when calculating the bandwidth consumed by it. The amount of networking flows consumed by the application is accounted with the Default Service. If there is any rate limit associated with Default Service BWC, this amount is accounted with Default Service BWC.

- No Cisco SCE Enforcement

No bandwidth control is enforced upon the subscribers. This results in unlimited bandwidth to the subscriber.

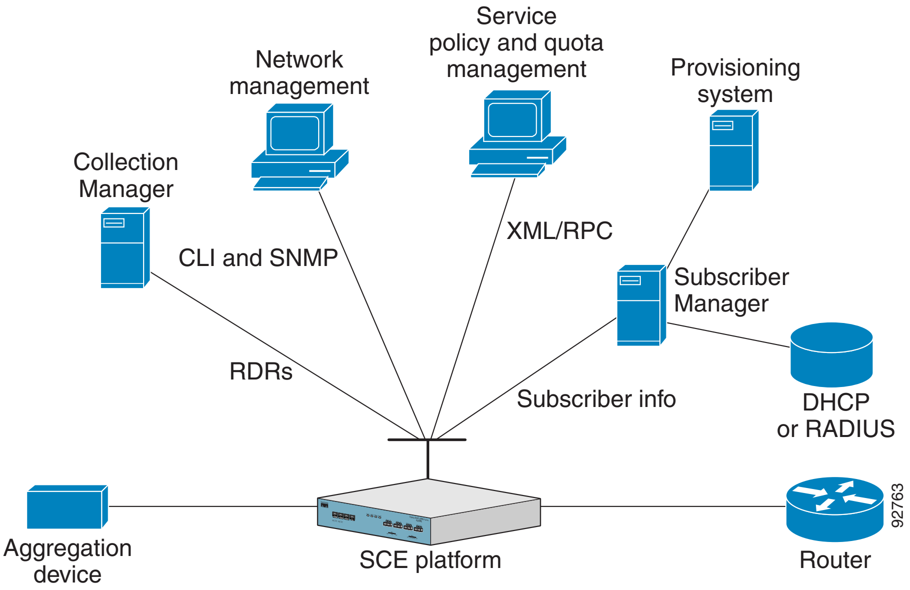
Management and Collection

The Cisco service control solution includes a complete management infrastructure that provides the following management components to manage all aspects of the solution:

- Network management
- Subscriber management
- Service Configuration management

These management interfaces are designed to comply with common management standards and to integrate easily with existing OSS infrastructure (Figure 1-2).

Figure 1-2 Service Control Management Infrastructure



Network Management

The Cisco service control solution provides complete network Fault, Configuration, Accounting, Performance, Security (FCAPS) Management.

Two interfaces provide network management:

- Command-line interface (CLI)—Accessible through the Console port or through a Telnet connection, the CLI is used for configuration and security functions.
- SNMP—Provides fault management (through SNMP traps) and performance-monitoring functionality.

Subscriber Management

Where the Cisco service control application for broadband (SCA BB) enforces policies on different subscribers and tracks usage on an individual subscriber basis, the Cisco service control management suite (SCMS) subscriber manager (SM) may be used as middleware software for bridging between OSS and Cisco SCE platforms. Subscriber information is stored in the SM database and can be distributed between multiple platforms according to actual subscriber placement.

The SM provides subscriber awareness by mapping network IDs to subscriber IDs. It can obtain subscriber information using dedicated integration modules that integrate with AAA devices, such as RADIUS or DHCP servers.

Subscriber information may be obtained in one of two ways:

- Push Mode—The SM pushes subscriber information to the Cisco SCE platform automatically upon logon of a subscriber.
- Pull Mode—The SM sends subscriber information to the Cisco SCE platform in response to a query from the Cisco SCE platform.

Service Configuration Management

Service configuration management is the ability to configure the general service definitions of a service control application. A service configuration file containing settings for traffic classification, accounting and reporting, and control is created and applied to a Cisco SCE platform. The SCA BB application provides tools to automate the distribution of these configuration files to Cisco SCE platforms. This standards-based approach makes it easy to manage multiple devices in a large network.

Service Control provides a GUI to edit and create these files and a complete set of APIs to automate their creation.

Data Collection

Data collection occurs as follows:

1. All analysis and data processing functions of the Cisco SCE platform result in the generation of Raw Data Records (RDRs), which the Cisco SCE platform forwards using a simple TCP-based protocol (RDR-Protocol).
2. RDRs are processed by the Cisco service control management suite collection manager.
3. The collection manager software is an implementation of a collection system that receives RDRs from one or more Cisco SCE platforms. It collects these records and processes them in one of its adapters. Each adapter performs a specific action on the RDR.

RDRs contain a variety of information and statistics, depending on the configuration of the system. Three main categories of RDRs include:

- Transaction RDRs—Records generated for each *transaction*, where a transaction is a single event detected in network traffic. The identification of a transaction depends on the particular application and protocol.
- Subscriber Usage RDRs—Records generated per subscriber, describing the traffic generated by that subscriber for a defined interval.
- Link RDRs—Records generated per link, describing the traffic carried over the link for a defined interval.

IPv6 Support

The Cisco SCE 8000 devices support processing of IPv6 traffic. The features that are available for IPv4, such as traffic processing, application classification and control, and management APIs, are available for IPv6 too.

The Cisco SCOS enhances the IPv6 capabilities of Cisco SCE 8000 devices by providing support to both IPv4 and IPv6 traffic simultaneously on all traffic processors.

Supported IPv6 features:

- Subscriber awareness.
- Virtual Gi
- Subscriber based classification for IPv6 traffic.
- Subscriber based bandwidth control.
- Content filtering for IPv6 traffic flows.
- Dual stack support on all traffic processors.
- Reporting and monitoring of IPv6 traffic.
- Support for IPv6 Fragmentation and Zones.
- IPv6 bundling support in DS-lite.
- Introduce IPv6 subscribers through Gx.
- Raw Data Records, except Attack RDRs and Malicious Traffic RDRs, are enhanced for IPv6.

  Redirection and blocking of traffic passing through 6to4, 6rd, and DS-Lite tunnels.

Cisco SCE devices work on three different system modes, namely, IPv4 only mode, IPv6 only mode, and dual stack mode. The default mode is dual stack mode. To configure the system mode, see the "Configuring the System Mode" section on page 3-17.

The following limitations are applicable to the IPv6 features on Cisco SCE Release 4.0.x:

- IPv6 addresses for connectivity to the management interfaces are not supported.
- Tunneling—The L2TP, GRE, GTP, MPLS, MPLS-VPN tunnels are not supported.
- Flow filter limitations:
  - For TCP flags, the PSH and URG fields are not considered, but SYN, ACK, RST, and FIN are considered.
  - Range options are not provided for subscriber side IP and network side IP address; instead, prefix length is used.
  - Inverse support is not provided for any of the fields.
- Value-Added Services (VAS) are not supported.
- Service classification and global bandwidth control are applicable for both IPv4 and IPv6. For example, there is only one browsing service for both IPv6 and IPv4 browsing traffic. Allocating the global bandwidth controller to a certain service limits the IPv6 and IPv4 traffic within that service.
- The Services over IPv6 are classified under the same service IDs as the corresponding services over IPv4.
- Flow capture is not supported for IPv6.

- Cisco SCE 8000 supports a maximum of 1M subscriber range. This means that the Cisco SCE can support a maximum of 1M subscribers with one mapping (either IPv4 or IPv6). But when the dual stack mode is enabled and all subscribers are dual stack subsribers—subscribers with one IPv4 and one IPv6 address, then the device supports only upto 500,000 dual stack subscribers.
- Cisco SCE 8000 devices identifies the IPv6 subscribers based on the MSB 64 bits of the subscriber IPv6 address. Cisco SCE 8000 devices support IPv6 subscribers within a range /32 to /64 and not less than /32.
- Virtual Gi is supported only in standalone configuration and not in cascade configuration.