QUICK START GUIDE

Cisco Service Control Product Installation Guide, Release 3.7.x

Revised: August 22, 2012, OL-24175-01

Note This document supports all 3.7.x releases.

1 Overview of the Cisco Service Control Solution

This section introduces the components of the Cisco Service Control solution and gives a high-level explanation of the entire installation process.

Cisco Service Control Components

The Cisco Service Control solution consists of five main components:

- Cisco Service Control Engine (SCE) platform—A flexible, powerful, and dedicated network-usage monitor that is custom-built to analyze and report on network transactions at the application level.

  For complete information about the installation and initial configuration of the Cisco SCE platform, see the *Cisco SCE Platform Installation Guides and Configuration Guides*.

- Cisco Service Control Application for Broadband (SCA BB)—An application that creates a service configuration file containing settings for traffic classification, accounting, and reporting, and applies it to a Cisco SCE platform. Cisco SCA BB provides tools to automate the distribution of these configuration files to Cisco SCE platforms. This simple, standards-based approach makes it easy to manage multiple devices in a large network.

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

- Service Control Management Suite (SCMS) Subscriber Manager—A middleware software component used when dynamic binding of subscriber information and policies is required. The Subscriber Manager manages subscriber information and provisions it in real time to multiple Cisco SCE platforms. The Subscriber Manager stores subscriber policy information internally, and acts 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 Subscriber Manager, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

  Quota Manager is an optional component of the Subscriber Manager. It enables Cisco 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 Service Control Management Suite Quota Manager User Guide*.

  Virtual Link Manager (VLM) is a component of the Subscriber Manager that enables Cisco Service Control solution providers to monitor and control individual subscriber links separately. For this, VLM creates a single policy with tier-differentiated packages, as also a number of virtual links, and then assigns subscribers to these virtual links. For more information, see the *Cisco Service Control for Managing Remote Cable MSO Links Solution Guide*.

- SCMS Collection Manager—Implementation of a collection system that receives Raw Data Records (RDRs) from one or more Cisco SCE platforms. The Collection Manager 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*.

- Service Control Application 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 Cisco SCA BB Console.

  For more information about the installation and operation of the SCA Reporter, see the *Cisco SCA BB Reporter User Guide*.

Together, the Cisco SCE platform, the SCMS Collection Manager, the SCMS Subscriber Manager, and the SCA Reporter or Cisco Insight are designed to support detailed classification, analysis, reporting, and control of IP network traffic. The SCMS Collection Manager, the SCA Reporter, and the SCMS Subscriber Manager are optional components; not all deployments of the Cisco Service Control solution require them. The following sites may not require all these components:

- Sites that employ third-party collection and reporting applications
- Sites that do not require dynamic subscriber-aware processing
- Sites that use a RADIUS or DHCP sniffing option.

Options and Versions

The Cisco SCE Platform

The Cisco SCE platform is available in three versions:

- SCE 1000—With two Gigabit Ethernet (GBE) interfaces, supporting one traffic link.
- SCE 2000 4xGBE—With four GBE interfaces, supporting two traffic links and cascaded topology.
- SCE 8000—With two or four 10 GBE interfaces. The four interfaces support two traffic links and cascaded topology.
  - SCE 8000—With eight or 16 GBE interfaces. The 16 interfaces support eight traffic links and cascaded topology.

All platform versions are available with either AC or DC power.

Note In general, this guide contains instructions for installing the Cisco SCE 8000 platform.

The Cisco SCA BB Application

Cisco SCA BB is not available in different versions.

Subscriber Manager

The SCMS Subscriber Manager is available in these versions:

- Solaris
- Linux

Both SCMS Subscriber Manager versions are available with these options:

- Optional Veritas cluster support for redundancy
- Optional Login Event Generators (LEGs)

Collection Manager

The SCMS Collection Manager is available in these versions:

- Solaris
- Linux

Both SCMS Collection Manager versions are available with either of these options:

- Uses the bundled database (Sybase Adaptive Server Enterprise database)
- Uses an external database (Any JDBC-compliant database, such as Oracle or MySQL, used with the JDBC Adapter)

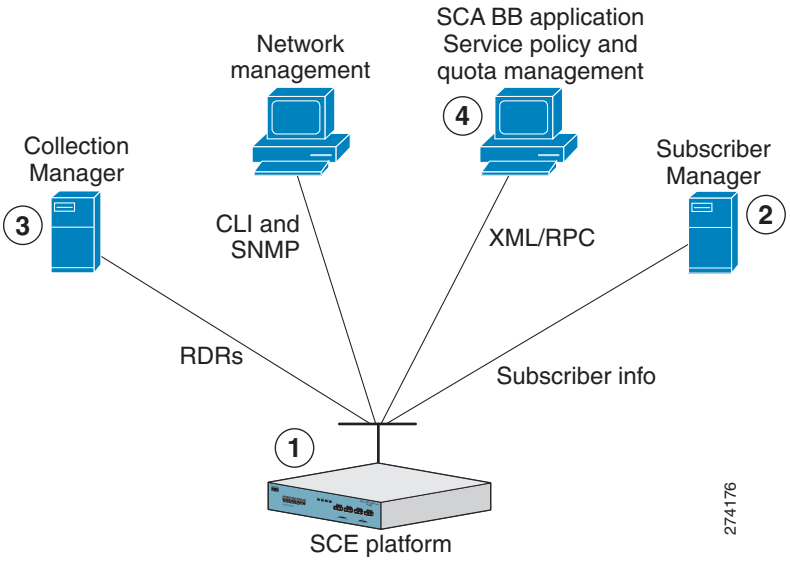
SCA Reporter

The Reporter is not available in different versions.

System Installation Overview

Figure 1 shows the order of in which the Cisco Service Control solution must be installed.

Figure 1 Installing the Complete Cisco Service Control Solution



To install the complete Cisco Service Control solution, complete these steps:

Step 1 Install the Cisco SCE platform (see the "Installing the Cisco SCE 8000 Platform" section on page 12).

This task includes:

- Installation in the rack
- Initial configuration by using a local console
- Cabling management and line ports

Step 2 Install the Subscriber Manager (see the "Installing the Subscriber Manager" section on page 14).

This task includes:

- Preliminary configuration (memory settings and configuration file.)
- Installing the SCMS Subscriber Manager software
- Adding a user for Proprietary Remote Procedure Call (PRPC) authentication

Step 3 Install the Collection Manager (see the "Installing the Collection Manager" section on page 16).

This task includes:

- (If using the bundled database) Installing the bundled database
- Installing the SCMS Collection Manager software
- Configuration related to the various adapters
- Adding a user for PRPC authentication
- (If using an external or unbundled database) Configuring the SCMS Collection Manager to be able to connect to the database

Step 4 Install the Cisco SCA BB Console and optional Cisco SCA BB configuration utilities (see the "Installing the Cisco SCA BB Application" section on page 20).

Step 5 Install the Cisco SCA BB application component (PQI file) and protocol pack on the Cisco SCE platform (see the "Installing the Application and Protocol Pack on the Cisco SCE Platform" section on page 22).

Step 6 Perform additional initial configuration, if any, of the Cisco SCE 8000 platform from the management workstation (see the "Initial Configuration of the Cisco SCE 8000 Platform" section on page 33).

Step 7 Perform initial configuration of the Cisco SCA BB application by using the Usage Analysis wizard (see the "Initial Cisco SCA BB Configuration" section on page 34).

2 Cisco Service Control Solution Topology

This section describes the possible deployment topologies of the Cisco Service Control solution.

Note This section presents the deployment topologies for the Cisco SCE 8000 platform. For information regarding the deployment topologies for the Cisco SCE 2000 platform, see the "Cisco SCE 2000 Platform Installation" section on page 49.

Overall System Topology

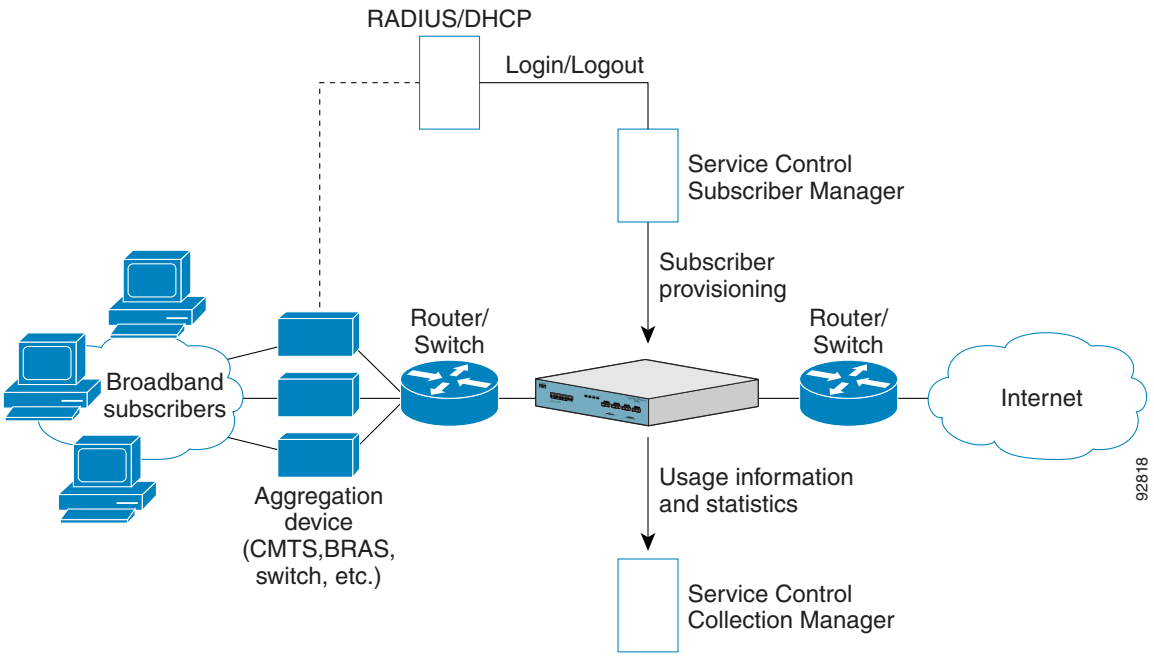
Figure 2 illustrates the general topology of the Cisco Service Control solution.

- Horizontal flow—Represents traffic between subscribers and an IP network.

  The SCE platform monitors traffic flow.
- Vertical flow—Represents transmission of RDRs from the Cisco SCE platform to the SCMS Collection Manager.

  The SCMS Subscriber Manager provides subscriber data. This flow allows Cisco SCA BB to conduct subscriber-level analysis and control.

Figure 2 Flow of Information in SCA BB



Cisco SCE 8000 Platform Topologies

The Cisco SCE 8000 platform is an ideal solution for dual links with load sharing and asymmetrical routing and support for fail-over between two Cisco SCE platforms.

Cisco SCE 8000 is built to support wire-speed processing of full-duplex 10 GBE streams. The Cisco SCE 8000 can, therefore, be deployed in a multilink environment, in several topologies:

- Single Cisco SCE 8000 topology—Enables processing of both upstream and downstream paths of a bidirectional flow, even if these paths traverse different links.
- Dual Cisco SCE 8000 topology (cascade)—Provides high-availability and fail-over solution, and maintains the line and service in case of Cisco SCE 8000 failure.
- Multi-Gigabit Service Control Platform (MGSCP) topology—Provides scalability. The Cisco SCE 8000 platform supports the option to connect multiple SCE platforms to a Cisco 7600 Series Router to perform load balancing between the platforms.

Physical Topologies

These are the descriptions of the physical topologies that Cisco SCE 8000 supports:

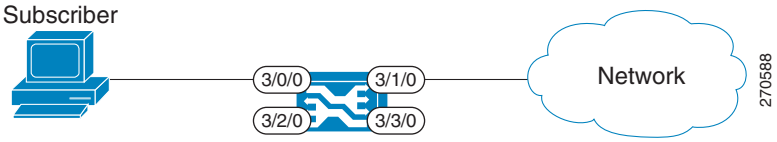
Single Cisco SCE 8000 Topologies

A single Cisco SCE 8000 supports both single 10GBE link and dual 10GBE link topologies.

Single Link: Inline Topology

Typically, Cisco SCE 8000 is connected in a full-duplex 10GBE link between two devices (Router, broadband remote access server, and so on). When Cisco SCE 8000 is installed inline, it physically resides on the data link between the subscribers and the network (see Figure 3).

Figure 3 Single Link: Inline Topology



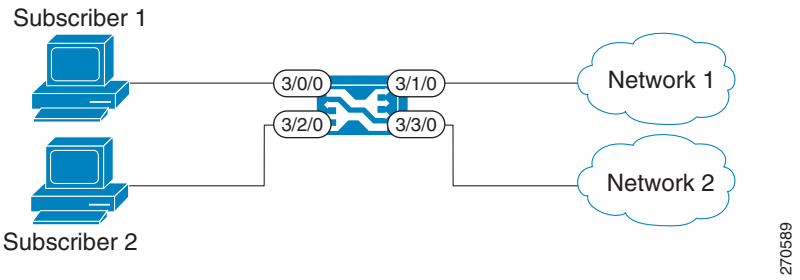
Dual Link: Inline Installation

In this topology, a Cisco SCE 8000 is connected inline in two full-duplex, 10GBE links (see Figure 4).

If load sharing exists between two links, asymmetrical routing might occur, and some of the flows may be split, that is, the upstream packets of the flow go on one link, and the downstream packets go on the other link.

When installed in this topology, Cisco SCE 8000 completely overcomes this phenomenon, and provides its normal functionality as if there is no asymmetrical routing in the two links.

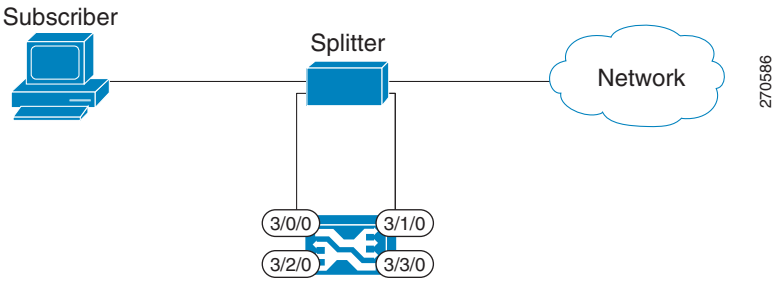
Figure 4 Dual Link: Inline Installation



Single Link: Receive-Only Topology

In this topology, an optical splitter resides physically on the 10GBE link between the subscribers and the network (see Figure 5). The traffic passes through the optical splitter, which splits the traffic to Cisco SCE 8000. As a result, Cisco SCE 8000 only receives traffic and does not transmit.

Figure 5 Single Link: Receive-Only Topology



In an optical splitter topology, Cisco SCE 8000 enables only the traffic monitoring functionality.

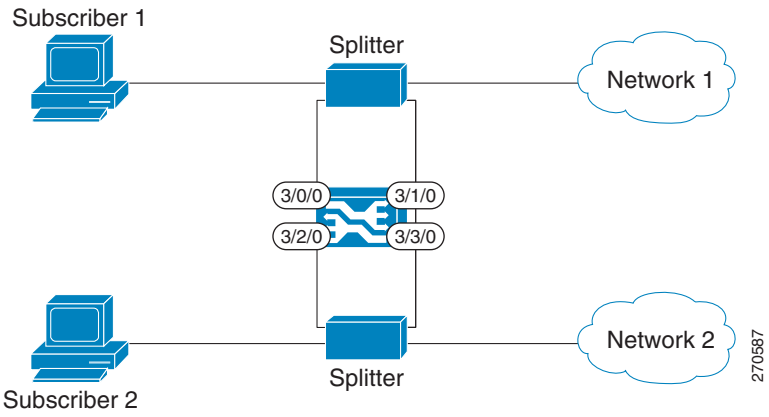
Note When implementing receive-only topologies with a switch, the switch must support the SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN ports destinations.

Dual Link: Receive-Only Topology

In this topology, a Cisco SCE 8000 is connected in receive-only mode to two full-duplex, 10 GBE links by using optical splitters (see Figure 6).

As with the dual link, inline topology, this topology completely overcomes the problem of asymmetrical routing.

Figure 6 Dual Link: Receive-Only Topology



Note When implementing receive-only topologies with a switch, the switch must support the SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN ports destinations.

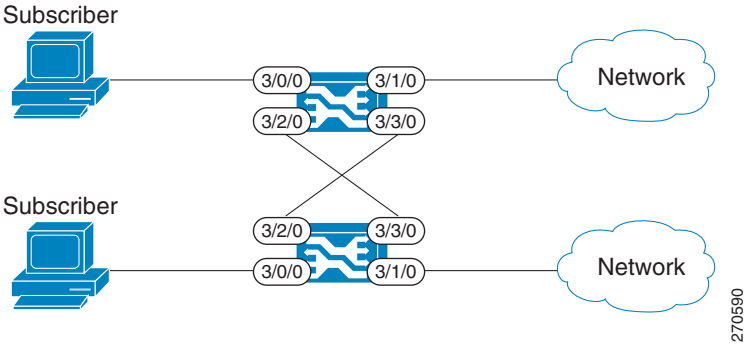
Dual Cisco SCE 8000 Topology (Cascade)

In this topology, two cascaded Cisco SCE 8000s are used. This topology allows a failover solution. If one Cisco SCE 8000 fails, the redundant platform preserves the functionality that Cisco SCE 8000 provides (see Figure 7).

This topology allows control and monitoring functionality, where redundancy is required and inline connection is used. The primary Cisco SCE 8000 processes the traffic of the two links, whereas the secondary Cisco SCE 8000 only bypasses the traffic of its links to the primary Cisco SCE 8000 for processing, and then bypasses the processed traffic back to the link. The two Cisco SCE 8000s also exchange keep-alive messages and subscriber state information.

If the primary Cisco SCE 8000 fails, the two Cisco SCE 8000s switch their roles, and failover is provided.

Figure 7 Two Cascaded Cisco SCE 8000 Platforms



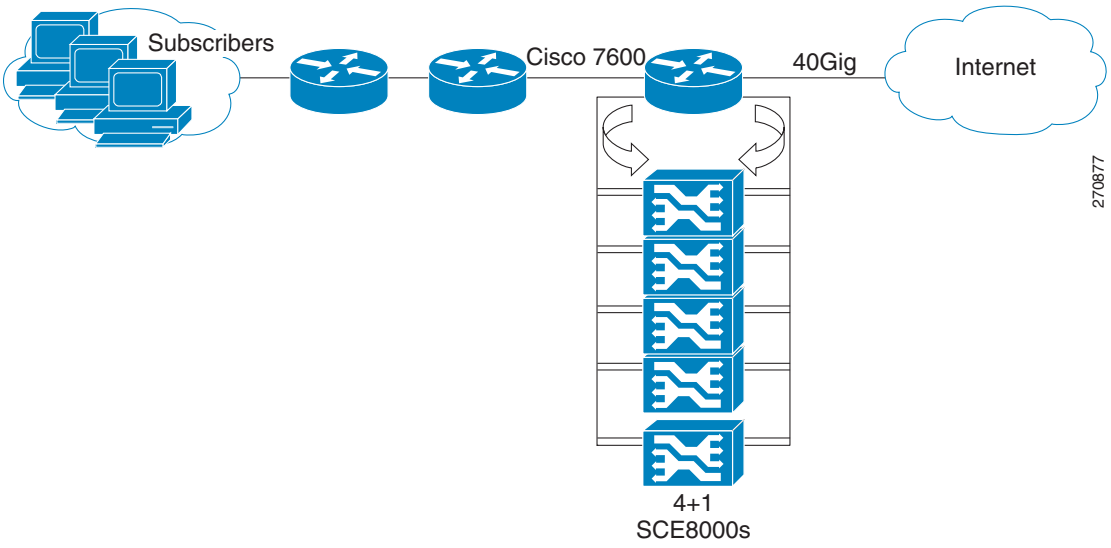
This failover solution preserves the Cisco SCE 8000 functionality and the network link:

- Two Cisco SCE 8000s are simultaneously synchronized about the subscriber contexts. Subscriber states are constantly exchanged between them, such that if the primary Cisco SCE 8000 fails, the secondary one can take over with minimum state loss.
- When one Cisco SCE 8000 fails, depending on the type of failure, its link traffic is still bypassed to the functioning Cisco SCE 8000 and processed there, so that traffic processing continues for both the links.
- You can configure the bypass of traffic through the failed Cisco SCE 8000, and choose to always cut off the line that goes through the failed Cisco SCE 8000. In such a scenario, network redundancy protocols, such as Hot Standby Router Protocol (HSRP), are responsible for identifying the line cutoff and switching the traffic such that it goes through the functioning Cisco SCE 8000.
- You can configure Cisco SCE 8000 to use an external optical bypass device so that if it fails, the bypass device is used to provide link continuity. This configuration ensures 100 percent link continuity at the expense of providing asymmetric routing functionality.

Multi-Gigabit Service Control Platform (MGSCP) Topology

In this topology, multiple Cisco SCE 8000 platforms are connected to a Cisco 7600 Series router, which acts as a dispatcher between the platforms (see Figure 8). The router contains two EtherChannels (ECs), one for the subscriber side and one for the network side, that perform load balancing for the Cisco SCE platform traffic. Traffic enters the first router, is distributed between the Cisco SCE platforms by the subscriber-side EC, and then returns to the router so that it can be forwarded to its original destination.

Figure 8 Basic MGSCP Topology



There are a number of variables to be considered in the MGSCP topology, two of which include:

- Type of SCE Platform Redundancy, page 10
- Redundant Cisco 7600 Series Router, page 11

Type of SCE Platform Redundancy

There are two types of SCE platform redundancy:

- All Active

  All the ports in the EtherChannel and all the Cisco SCE platforms are active. If a failure occurs on one of the Cisco SCE platforms, the links on the related ports in the EC go down and the EC automatically excludes them from load distribution. The load is then distributed among the active Cisco SCE platforms.

  Because Cisco SCE 8000 supports two links, this configuration requires one Cisco SCE platform per two links (two EC ports).

- N+1

  N Cisco SCE platforms are active and one platform is on standby. The EC ports connected to the standby Cisco SCE platform must be configured as standby ports. If one Cisco SCE platform fails, the EtherChannel ports connected to the failing SCE platform are shut and the standby EtherChannel ports, connected to the standby SCE platform are activated.

  Because Cisco SCE 8000 supports two links, this configuration requires one SCE platform per two links (two EtherChannel ports), plus one extra SCE platform for standby.

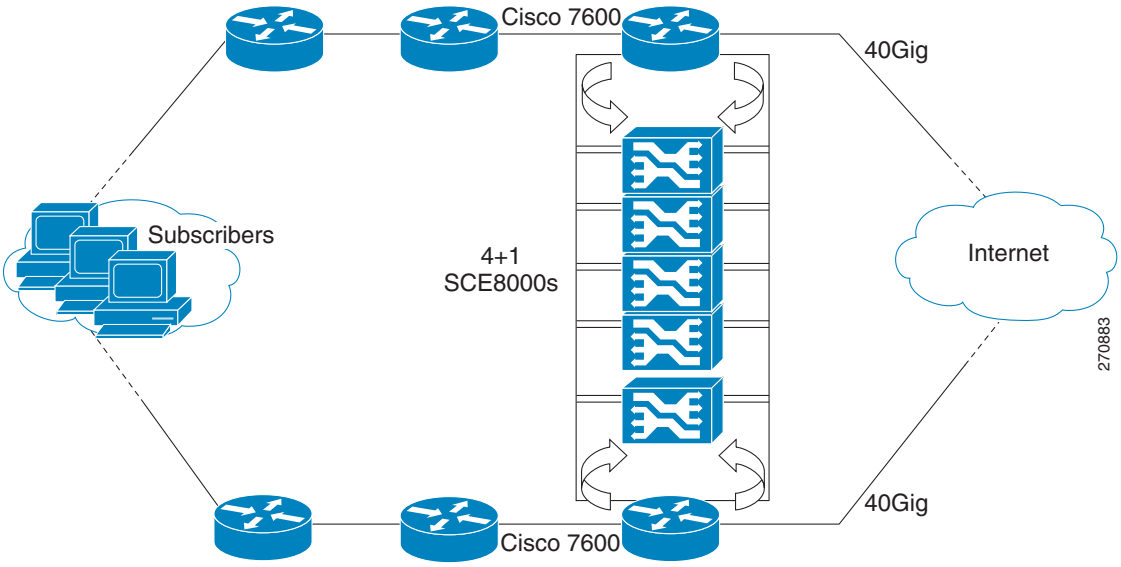
Note The standby SCE platform must be connected to the two highest-numbered ports, because EC behavior automatically designates these ports as the standby ports.

Redundant Cisco 7600 Series Router

Two Cisco 7600 Series routers can be used to provide network redundancy (see Figure 9).

In this topology, one link on each Cisco SCE 8000 platform is connected to each router. Therefore, one SCE platform is required for each link.

Figure 9 MGSCP with Redundant Router



3 System Installation

This chapter describes the system installation of the Cisco Service Control solution.

Installing the Cisco SCE 8000 Platform

To install the Cisco SCE 8000 platform, complete the following steps. (For more information, see the *Cisco SCE 8000 10GBE Installation* and *Configuration Guide* or the *Cisco SCE 8000 GBE Installation and Configuration Guide*.)

Note For information about installing an SCE 2000 platform, see the "Installing a Cisco SCE 2000 Platform" section on page 52.

Step 1 Install the Cisco SCE platform on the rack.

Step 2 Connect the chassis ground and the power.

Step 3 Connect the CON port to a local terminal. Configure the initial setup parameters as necessary. (See the "Initial Configuration of the Cisco SCE 8000 Platform" section on page 33).

Step 4 Connect the MNG port to the local LAN.

Step 5 Cable the line ports. (See the"Cisco SCE 8000 Connectivity" section on page 12 for a summary of proper cabling for various topologies).

Cisco SCE 8000 Connectivity

Table 1, Table 2, Table 3, Table 4, and Table 5 summarize Cisco SCE 8000 connectivity for the basic topologies.

Note Receive-only topologies use only Receive fibers. these can be implemented by using either an optical splitter or a switch. If a switch is used, it must support SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN ports destinations.

Table 1 Single-Link Inline Connectivity

Port	Link	Side
3/0/0	Link 0	Subscribers
3/1/0	Link 0	Network

Table 2 Dual-Link Inline Connectivity

Port	Link	Side
3/0/0	Link 0	Subscribers
3/1/0	Link 0	Network
3/2/0	Link 1	Subscribers
3/3/0	Link 1	Network

Table 3 Cascade Connectivity

This port on Cisco SCE 8000 #1	Connects to...
3/0/0	Subscriber-side network element
3/1/0	Network-side network element
3/2/0 (cascade port)	Port 3/3/0 on Cisco SCE 8000 #2
3/3/0 (cascade port)	Port 3/2/0 on Cisco SCE 8000 #2
This port on SCE8000 #2	**Connects to...**
3/0/0	Subscriber-side network element
3/1/0	Network-side network element
3/2/0 (cascade port)	Port 3/3/0 on Cisco SCE 8000 #1
3/3/0 (cascade port)	Port 3/2/0 on Cisco SCE 8000 #1

Table 4 Optical Bypass Connectivity: Single Link

Optical Bypass Port	Connects to...
A	Subscriber-side network element
B	Network-side network element
C	Cisco SCE platform port 3/0/0
D	Cisco SCE platform port 3/1/0
CTRL	Left-hand External Bypass port on the Cisco SCE 8000-SCM-E module.

Table 5 Optical Bypass Connectivity: Dual Link

Port on Optical Bypass #1	Connects to...
A	Subscriber-side network element
B	Network-side network element
C	Cisco SCE platform port 3/0/0
D	Cisco SCE platform port 3/1/0
CTRL	Left-hand External Bypass port on the Cisco SCE 8000-SCM-E module.
Port on Optical Bypass #2	**Connects to...**
A	Subscriber-side network element
B	Network-side network element
C	Cisco SCE platform port 3/2/0
D	Cisco SCE platform port 3/3/0
CTRL	Right-hand External Bypass port on the SCE 8000-SCM-E module.

MGSCP Topologies

In an MGSCP deployment, the exact cabling scheme depends on the number and arrangement of ports in the EtherChannel in the Cisco 7600 Series router. It is, therefore, not possible to provide exact cabling schemes.

The following general guidelines are applicable during the process of designing the cabling scheme:

- Because there are two links per Cisco SCE 8000 platform, the minimum number of platforms required is half the number of links used.
- Each link corresponds to one port on the EtherChannel on the Cisco 7600 Series router. Each EtherChannel supports a maximum of eight ports. Therefore, if all eight EtherChannel ports are configured, four Cisco SCE 8000 platforms are required.
- For N+1 redundancy, two ports (connected to the standby platform) must be configured as standby ports on both EtherChannels. Therefore, for N+1 redundancy, one router and five Cisco SCE 8000 platforms will be used to support eight links.
- If two Cisco 7600 Series routers are used (for network redundancy), one link on each Cisco SCE 8000 platform is connected to each router. This topology requires twice the number of Cisco SCE 8000 platforms, one platform for each link.
  - A minimum of eight Cisco SCE 8000 platforms are required to support eight ports.
  - For N+1 redundancy, nine Cisco SCE 8000 platforms are used to support eight active links.

When cabling to the EtherChannel, follow these guidelines:

- The Cisco SCE platform ports *must* be connected to the EtherChannel ports in the same order on both sides.
- The EtherChannel ports *must* be sorted in ascending order by their physical interface numbers.
- In a topology with two Cisco 7600 Series routers, the order of connection to the EtherChannel ports *must* be the same on both routers. For both routers to send the traffic of a given subscriber to the same Cisco SCE platform, the Cisco SCE platforms must be connected to both routers in the same order (one Cisco SCE platform connected to the first link on both routers, another Cisco SCE platform connected to the second link on both routers, and so on).

Installing the Subscriber Manager

This section describes how to install Subscriber Manager, Release 3.7.0, on a computer running Solaris or Red Hat Linux.

For more information, see the *Cisco SCMS Subscriber Manager User Guide*.

To install Subscriber Manager, Release 3.7.0, complete these steps:

Step 1 Use FTP to load the distribution files to the Subscriber Manager and extract them.

Step 2 Determine the system memory settings.

Set the system memory configuration requirements according to the maximum number of subscribers. See the "Installation Procedure" section in the "Installation and Upgrading" chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Step 3 Configure the shared memory settings.

TimesTen requires that certain changes be made in the OS kernel configuration file:

- For Solaris, modify the /etc/system file.
- For Linux, modify the /etc/sysctl.conf file.

These changes increase the shared memory and semaphore resources on the machine from their defaults. See the "Installation Procedure" section in the "Installation and Upgrading" chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Step 4 (Optional) Edit the install-def.cfg file.

Note We recommend that you edit the install-def.cfg file if you do not want the default parameter values to be used.

The install-def.cfg file contains several parameters that can be configured before you install the Subscriber Manager. The installation routine copies these parameters to the relevant Subscriber Manager configuration file. By default, all the parameters are commented and the default values are used.

Table 6 lists the parameters of the install-def.cfg file.

Table 6 Parameters of the install-def.cfg File

Parameter Name	Resides In	Description	Alternate Configuration Option
max_subscribers_num	SM definitions	Defines the maximum number of subscribers that the Subscriber Manager supports. Maximum: • Solaris—20 million • Linux—2 million Default is 200,000.	The max_number_of_subscribers parameter in the p3sm.cfg configuration file.
sm_memory_size	SM definitions	Defines the amount of memory, in megabytes, that is allocated for the Subscriber Manager process.	The PCUBE_SM_MEM_SIZE in the sm.sh file that resides in the ~pcube folder.
database_perm_size	Database definitions	Defines the PermSize, in megabytes, allocated for the database.	The PermSize parameter in the /var/TimesTen/sys.odbc.ini file.
database_temp_size	Database definitions	Defines the TempSize, in megabytes, allocated for the database.	The TempSize parameter in the /var/TimesTen/sys.odbc.ini file.

Step 5 Execute the install-sm.sh script.

Note You can customize the install-sm.sh script.

Note If the /etc/motd file exists, it is *not* possible to run the script. Move or remove the /etc/motd file before you run the install-sm.sh script.

From your workstation shell prompt, move to the directory to which the distribution file was extracted and run the install-sm.sh script. See the "Installation Procedure" section of the "Installation and Upgrading" chapter of *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Step 6 Set the password for the pcube user.

After the installation script runs successfully, set the password for the pcube user by running the **# passwd pcube** command.

Note We recommend that you note down this password for future use.

Step 7 Reboot the computer. This step is mandatory to complete the installation.

Step 8 Add a user for PRPC authentication.

It is necessary to add a user for PRPC authentication because Cisco SCA BB requires a username and password when connecting to the Subscriber Manager.

To add a user for PRPC authentication, use the **p3rpc** command-line utility. For example:

```
>p3rpc --set-user --username=pcube --password=pcube-password
```

Installing the Collection Manager

This section describes how to install the Collection Manager, either with the bundled Sybase database or unbundled, on a computer running Solaris or Red Hat Linux:

- Ports Used by the Collection Manager Software, page 16
- Installing the Sybase Database, page 17
- Installing Collection Manager Software, page 17

For more information, see the *Cisco Service Control Management Suite Collection Manager User Guide*.

Ports Used by the Collection Manager Software

Table 7 describes the TCP/UDP ports on which the Collection Manager software and associated components (such as the Sybase database) listen. This table helps the network administrator understand the behavior of the software and its adherence to the security policy.

Table 7 Ports that the Collection Manager Listens on Constantly

Port Number	Description
33000	Used by the Cisco SCE devices to send RDRs for data collection.
21	Used by the legacy (releases earlier than 3.0) SCAS Reporter to authenticate against the Collection Manager user on the Collection manager machine.
33001	Internal collection manager. **Note** Access is required only from the local machine; external access can be blocked.
9092	HTTP technician interface.
4100	Sybase database connectivity through ODBC/JDBC (for installations with bundled Sybase). Required for access to the database.
1099—1120	RMI. Used as the management interface between the data collector and the Service Control management server.
22000	FTP server of the Collection Manager. **Note** FTP transactions may listen on other ports (22001 to 22100) for data transfer, as negotiated by the protocol.
7787	Internal logging of the management user log. **Note** Access is required only from the local machine; external access can be blocked.
14375	Used by the Cisco SCA BB Console to send symbol definitions (values.ini) to the Collection Manager.
33002	Internal Collection Manager for Cisco IOS Flexible NetFlow.
2055	The UDP port used by the Cisco ASR 1000 router to send Cisco ASR 1000 Flexible NetFlow records for data collection.
9093	HTTP technician interface for Cisco IOS Flexible NetFlow.
14376	Used by PRPC.

The ports that are listed are those ports on which the device listens constantly. Allow access on these port numbers; otherwise, certain operations may fail.

Some operations (such as file transfer) cause a device to open ports, other than those listed, temporarily; however, these ports close automatically after the operation ends.

Installing the Sybase Database

If you do not want to install Sybase (for example, when working in the unbundled mode), perform the task described in the "Installing Collection Manager Software" section on page 17.

Keep the following points in mind when using the Sybase database:

- Installing the Sybase database can take up to three hours.
- When using the bundled Sybase database, the server on which you install the Collection Manager can have a maximum of four CPU cores.
- The maximum database size supported by the bundled Sybase database is 50 GB. For database support larger than 50 GB, use an external database.

The **installsyb.sh** script installs the Sybase database. For information about the actions performed by the script, see the *Cisco Service Control Management Suite Collection Manager User Guide*.

Step 1 Log in as the root user and make the distribution kit contents available on your system or local network.

Step 2 In the distribution kit root, change directory to **sybase.**

Step 3 Run the **installsyb.sh** script as follows:

```
installsyb.sh --sybhome=SYBHOME {--datadir=DATADIR}
```

- SYBHOME is the home directory of the Sybase user. The Sybase home directory for Linux should have 2 GB free space and for Solaris 6 GB free space.
- Select the data location option by specifying:
  - Specify --datadir=DATADIR. Here, DATADIR is the directory in which all Sybase data is stored.

  Use a location in a partition where at least 30 GB free space is available.
- If you specify a DATADIR, all the Sybase data is stored as normal files in that directory, with default sizes of 20 GB for data, 6 GB for logs, and 2 GB for Sybase temporary storage. The ownership of the directory is changed to the Sybase user during installation.

Step 4 After the script completes, set a password for the sybase user. Use the **passwd** command as follows:

```
# passwd sybase
```

Installing Collection Manager Software

Use the **install-cm.sh** script to install the Collection Manager server.

install-cm.sh Options

The usage message for the **install-cm.sh** script is:

```
Usage: install-cm.sh [-h] (-d CMDIR | -o)

Options: -d CMDIR   select directory for ~scmscm
                 (must not exist and must be on 8 GB free partition)
         -o   upgrade the existing installation
              while preserving the current configuration
               (can't be used with -d)
         -h   print this help and exit
```

The description of the options is as follows:

```
-d CMDIR
          Used to designate the directory of the newly created
          scmscm user's home. Should be the name of a
          non-existing directory, whose parent resides on a
          partition where at least 8 GB is free.
          As an alternate to this option, you can specify -o :

 -o
          Use this option when you wish to upgrade the existing
          installation while preserving the current configuration.
              (can't be used with  -d)
```

For information about the actions performed by the **install-cm.sh** script, see the *Cisco Service Control Management Suite Collection Manager User Guide*.

Install the Collection Manager server by performing the following procedure:

Step 1 Change directory to **install-scripts** under the distribution kit root.

Step 2 Run the **install-cm.sh** script:

```
# install-cm.sh -d <CM home dir>
```

After running the script, a user-driven configuration manager presents the user with options for the basic configuration of the Collection Manager.

Step 3 Choose one of the options provided by the configuration manager:

```
Please select one of the following options:
1 - Install CM:RDR
2 - Install CM:NetFlow
3 - Install CM:RDR and CM:NetFlow
4 - Exit
```

- Choose option 1 if the Collection Manager is being configured to operate with Cisco SCE.
- Choose option 2 if the Collection Manager is being configured to operate with the Cisco ASR 1000 Series Aggregation Services Routers.
- Choose option 3 if the Collection Manager is being configured to operate with both Cisco SCE and the Cisco ASR 1000 Series Aggregation Services Routers.
- Choose option 4 is chosen to exit the Collection Manager installation.

Step 4 Choose whether to enable or not enable the real-time aggregating (RAG) adapter. For more information on the RAG adapter, see the *Cisco Service Control Management Suite Collection Manager User Guide*.

```
Do you want to enable the RAG Adapter? (yes/no):
```

Step 5 You can choose to set up the Collection Manager database at the time of installation or configure it at a later time.

```
Would you like to configure the database?: yes
```

Step 6 If you choose to configure the database:

a. Select the number corresponding to the relational database management system of the connecting database:

```
Enter the RDR DB type:
1 - Oracle
2 - MySQL
3 - Sybase
Enter your choice:
```

For more information, see the "Configuring Databases" section in the "Managing the Collection Manager" chapter of the *Cisco Service Control Management Suite Collection Manager User Guide*.

b. Enter the following server information or press **Enter** to leave at the default shown.

```
Enter DB server host (default localhost):
Enter DB server listening port (default port no) :
Enter DB server instance id (default schema) :
Enter DB schema user name (default user_id) :
Enter DB schema user password (default password) :
```

You will see the following text:

```
PASS:db is up
DB connection succeeded.
```

Note A failed connection results in the user being prompted to re-enter the DB information.

Note After the user configures the requested database options, the dbinfo.vm file updates for the RDR database configuration details, the Cisco IOS Flexible NetFlow database configuration details, or the configuration details of both the RDR database and the Cisco IOS Flexible NetFlow database.

Note We recommend that you set up separate databases for each platform.

Step 7 After the script completes running, set a password for the scmscm user:

```
passwd scmscm
```

We recommend that you maintain a record of the password.

Step 8 (Optional) To configure the Collection Manager to use an external database, use the **~scmscm/scripts/dbconf.sh -- rdr** script.

This is a list of supported external databases:

- Oracle—Releases 9.2, 10g, and 11g
- MySQL—Releases 4.1 and later
- Sybase—Version 12.5.1 and later

Step 9 Start the database.

If you are using an external database, start it according to the instructions supplied by the database vendor.

If you are using the Sybase database:

a. As the root user, run the **sybase start** command:

 # ~scmscm/setup/sybase start

b. Wait for several minutes and run the **alive.sh** script:

 # ~scmscm/setup/alive.sh

Make sure that the output does not contain the phrase *Sybase not functioning*.

Step 10 Configure the adapters to use and the categorizer.

For details, see the "Configuring the Collection Manager" section of the *Cisco Service Control Management Suite Collection Manager User Guide*.

Step 11 Set the Collection Manager time zone by using the **jselect-sce-tz.sh** script. For example, if the Cisco SCE device is located in GMT+2, run this command as the scmscm user:

```
$ ~scmscm/cm/bin/jselect-sce-tz.sh --rdr --offset=120
```

Step 12 Activate the periodic delete procedures for the database tables by running the **create_periodic_del_procs.sh** script as the scmscm user:

```
~scmscm/db_maint/create_periodic_del_procs.sh --rdr
```

For details, see the "Managing the Periodic Deletion of Old Records" section of the *Cisco Service Control Management Suite Collection Manager User Guide*.

Step 13 Activate the automatic invocation of the periodic delete procedures:

```
$~scmscm/scripts/dbperiodic.sh --rdr --load
```

This loads the default data retention settings defined in ~scmscm/db_maint/dbperiodic.conf.

Step 14 Start the Collection Manager by running this command:

~scmscm/cm/bin/cm start

Step 15 Add a user for PRPC authentication. It is necessary to add a user for PRPC authentication because Cisco SCA BB requires a username and password when connecting to the CM.

To add a user for PRPC authentication, use the **p3rpc** command-line utility:

```
~scmscm/cm/bin/p3rpc --set-user --username=scmscm --password=scmscm-password
```

Installing the Cisco SCA BB Application

This section describes how to install the Cisco SCA BB application.

For more information, see the *Cisco Service Control Application for Broadband User Guide*.

SUMMARY STEPS

Step 1 Ensure that both the Cisco SCE platforms and the Subscriber Manager operate and run on versions that are compatible with your Cisco SCA BB version.

Step 2 Install the Cisco SCA BB Console.

Step 3 (Optional) Install the Cisco SCA BB utilities:

- Service Configuration Utility (**servconf**)
- SCA BB Signature Configuration Utility (**sigconf**)
- SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd**) (together with associated real-time monitoring report templates).

Step 4 Install the Cisco SCA BB application component that resides on the Cisco SCE platform. This installation can be carried out from the Cisco SCA BB Console at a later stage in the overall installation process. See the "How to Install Files on the Cisco SCE Platform" section on page 23.

How to Verify that the Cisco SCE Platform is Running a Compatible Version of the OS

Step 1 From the Cisco SCE platform CLI prompt `(SCE#)`, type `show version`.

Step 2 Press **Enter.**

The response shows the version of the OS running on the Cisco SCE platform.

How to Verify that the Subscriber Manager is Running a Compatible Version

Step 1 Open a Telnet session to the Subscriber Manager.

Step 2 Go to the Subscriber Manager bin directory and enter `p3sm version`.

Step 3 Press **Enter.**

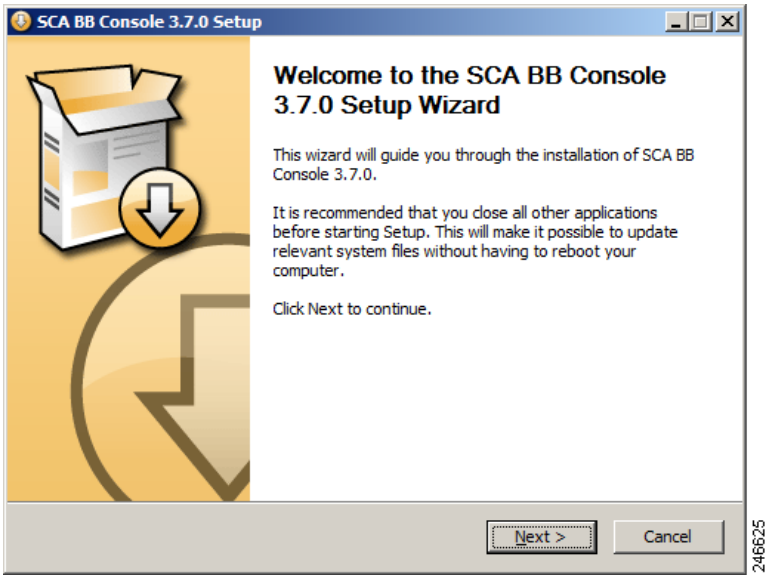
The response to this command displays the Subscriber Manager version.

How to Install the Cisco SCA BB Console

Step 1 Navigate to the Console installation file, sca-bb-console-<xxx>.exe, and double-click it.

A standard installer wizard appears (see Figure 10).

Figure 10 SCA BB Console 3.7.0 Setup Wizard



Step 2 Follow the standard installation steps to install the application at the desired location.

How to Install the Cisco SCA BB Configuration Utilities

Installing the Cisco SCA BB configuration utilities is optional.

Step 1 From the Cisco SCA BB installation package, extract the scas_bb_util.tgz file, and copy it to a Windows, Solaris, or Linux workstation.

Step 2 Unpack the file to a new folder.

These files are in the bin directory:

- SCA BB Service Configuration Utility (servconf)
- SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd**) and associated real-time monitoring report templates

Installing the Application and Protocol Pack on the Cisco SCE Platform

Use the Cisco SCE Software Upgrade wizard in the console to install the application file (PQI) and the protocol pack (SPQI) on selected Cisco SCE platforms.

Before You Start

Before you begin the Cisco SCE platform upgrade, ensure that you perform the following tasks:

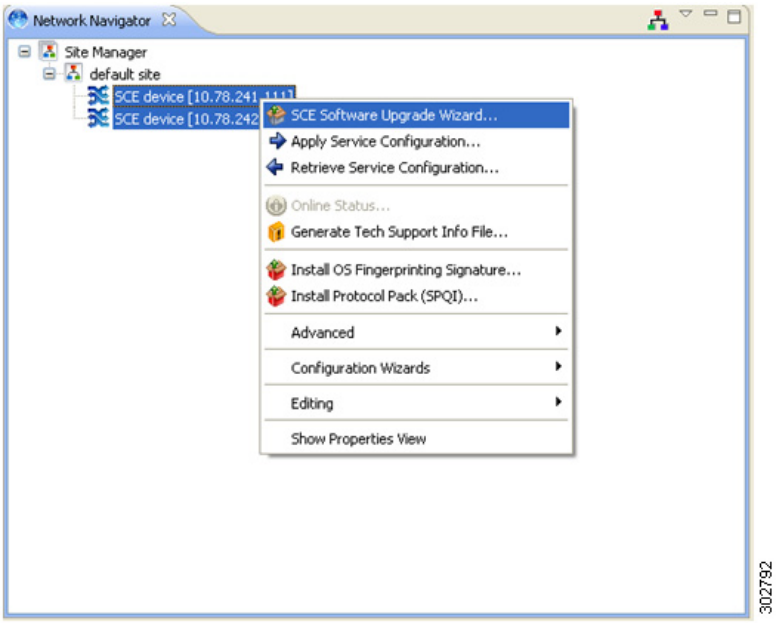
- If the IP addresses of the Cisco SCE platforms to be upgraded are not defined in the Network Navigator, gather the IP addresses of all SCE platforms to be upgraded.
- Download the relevant PQU file and protocol pack to a local location or to a location accessible by FTP. If using an FTP site, make sure you have the complete FTP location and path for each file.

How to Install Files on the Cisco SCE Platform

Step 1 In the Network Navigator of the console, select the Cisco SCE platforms to be upgraded. Right-click the corresponding Cisco SCE platform name and choose **SCE Software Upgrade Wizard** (see Figure 11).

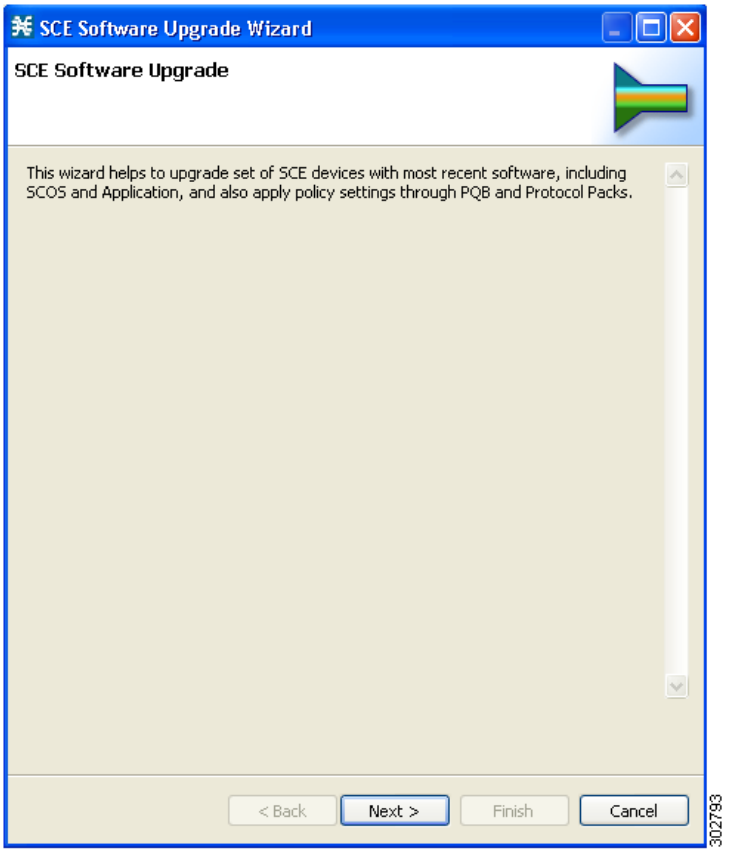
If the Cisco SCE platforms are not yet defined in the Network Navigator, you can select the site node.

Figure 11 Network Navigator



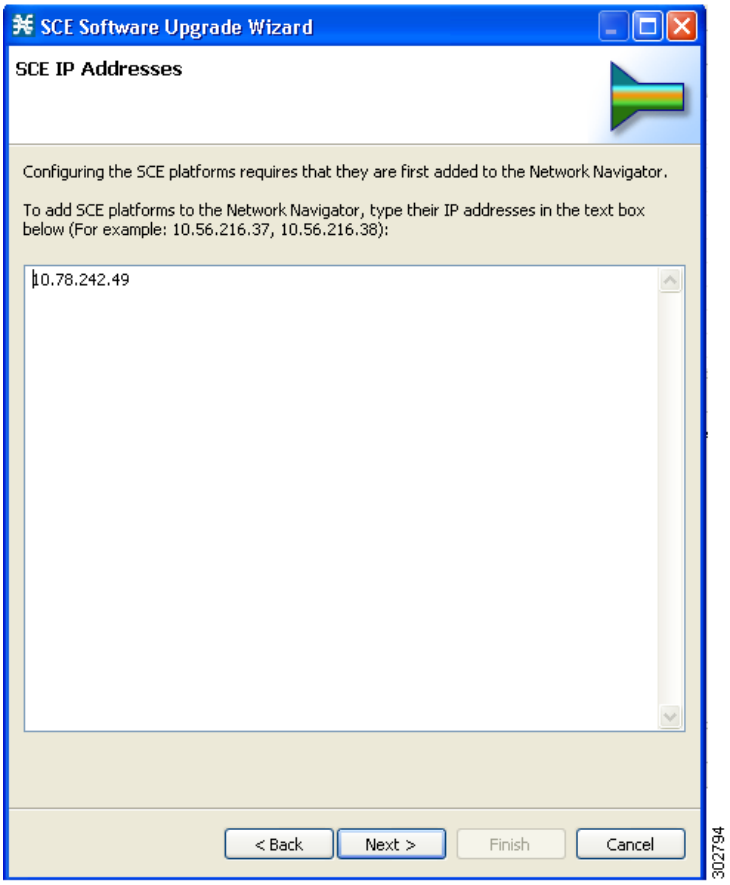
The SCE Software Upgrade Wizard opens. Click **Next**(see Figure 12).

Figure 12 SCE Software Upgrade Wizard



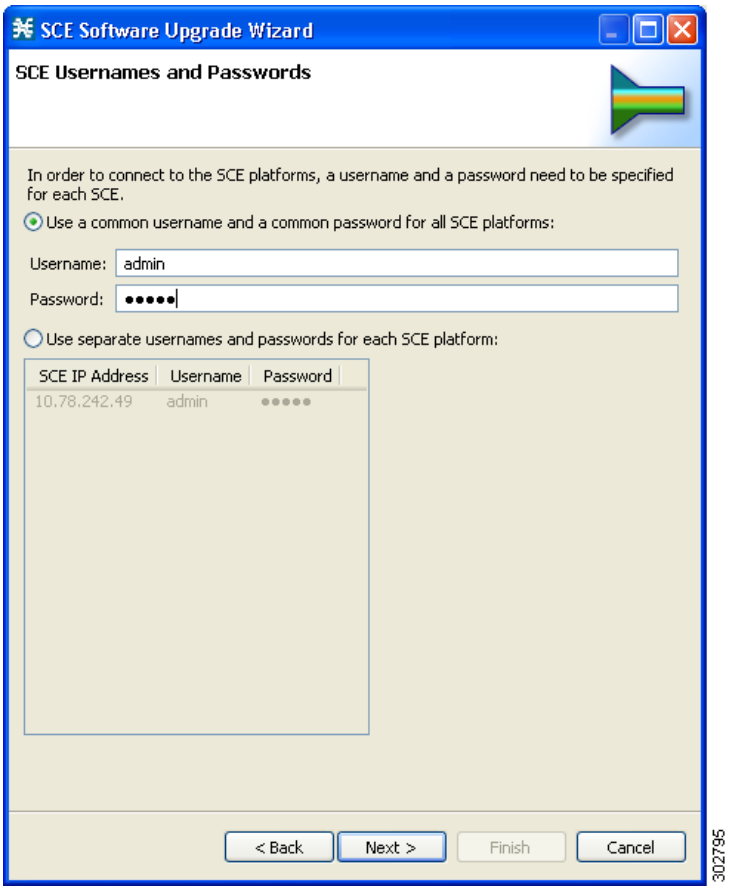
Step 2 In the SCE IP Addresses pane (see Figure 13), verify that the IP addresses of all the Cisco SCE platforms to be upgraded are displayed. If any of the IP addresses are not displayed, enter the details and click **Next**.

Figure 13 SCE Software Upgrade Wizard—SCE IP Addresses



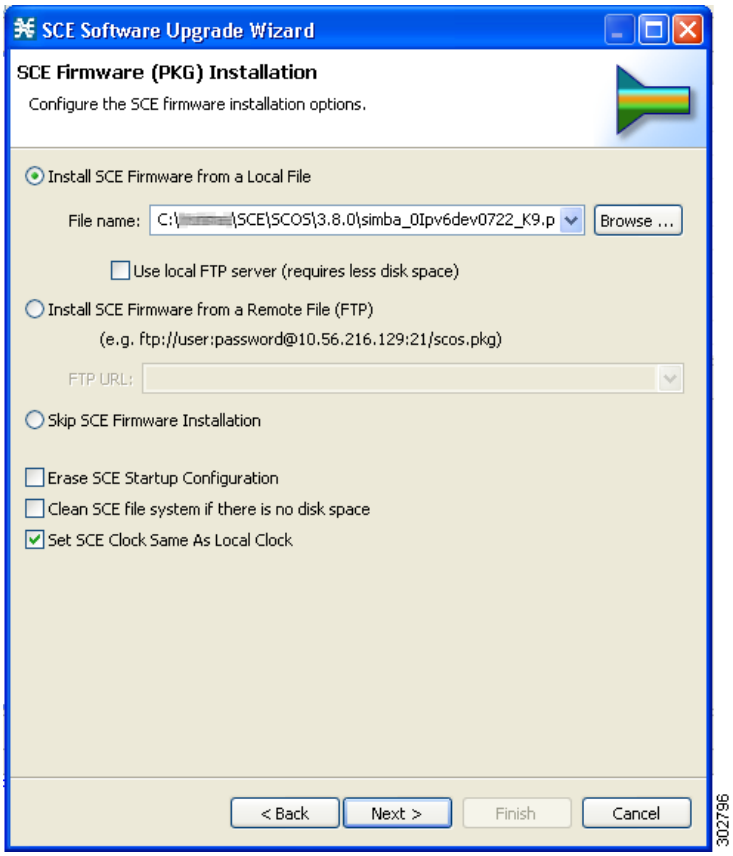
Step 3 In the SCE Usernames and Passwords pane (see Figure 14), enter the username and password required to access the Cisco SCE platform. You can use the same username and password for all the platforms or enter a different username and password for each platform and click **Next**.

Figure 14 SCE Software Upgrade Wizard—SCE Usernames and Passwords Window



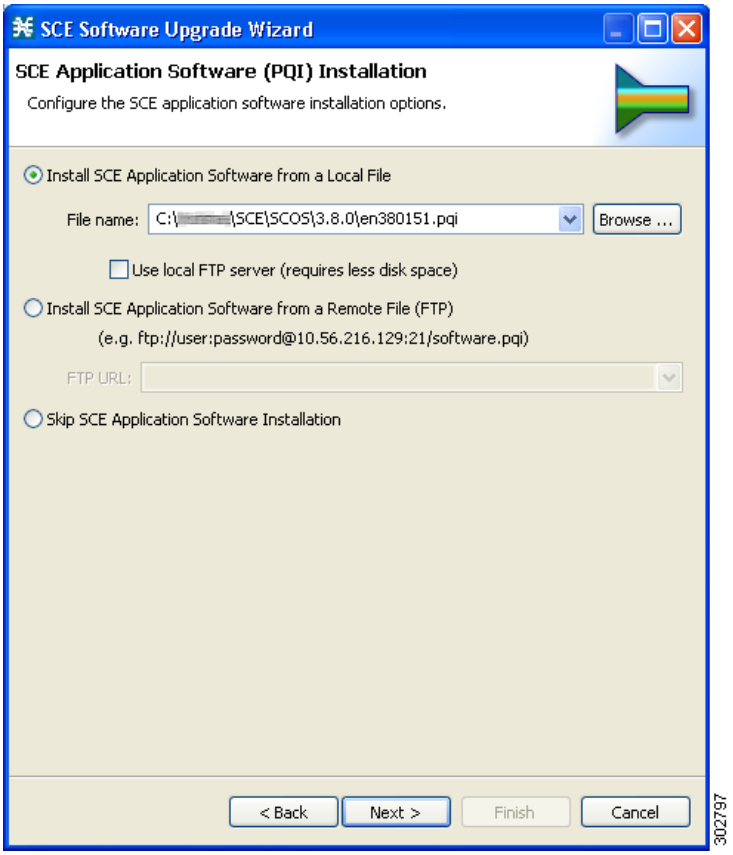
Step 4 In the SCE Firmware (PKG) Installation pane (see Figure 15), specify the location of the firmware file to be installed on all the selected Cisco SCE platforms and click **Next**.

Figure 15 SCE Software Upgrade Wizard—SCE Firmware (PKG) Installation



Step 5 In the SCE Application Software (PQI) Installation pane (see Figure 16), specify the location of the PQI file to be installed on all the selected Cisco SCE platforms and click **Next**.

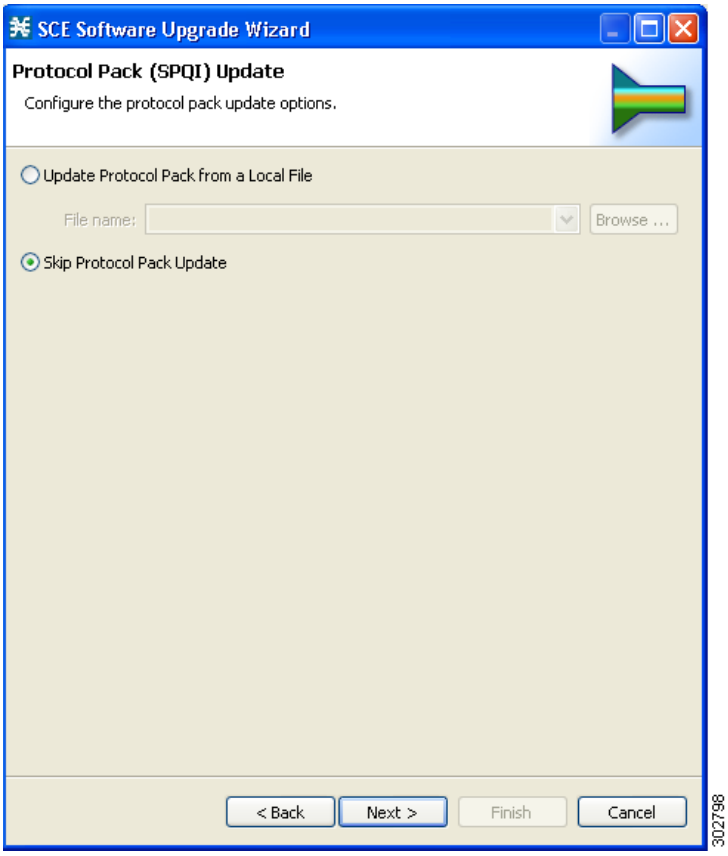
Figure 16 SCE Software Upgrade Wizard—SCE Application Software (PQI) Installation



Step 6 In the Protocol Pack (SPQI) Update pane (see Figure 17), check Skip Protocol Pack Update and click **Next**.

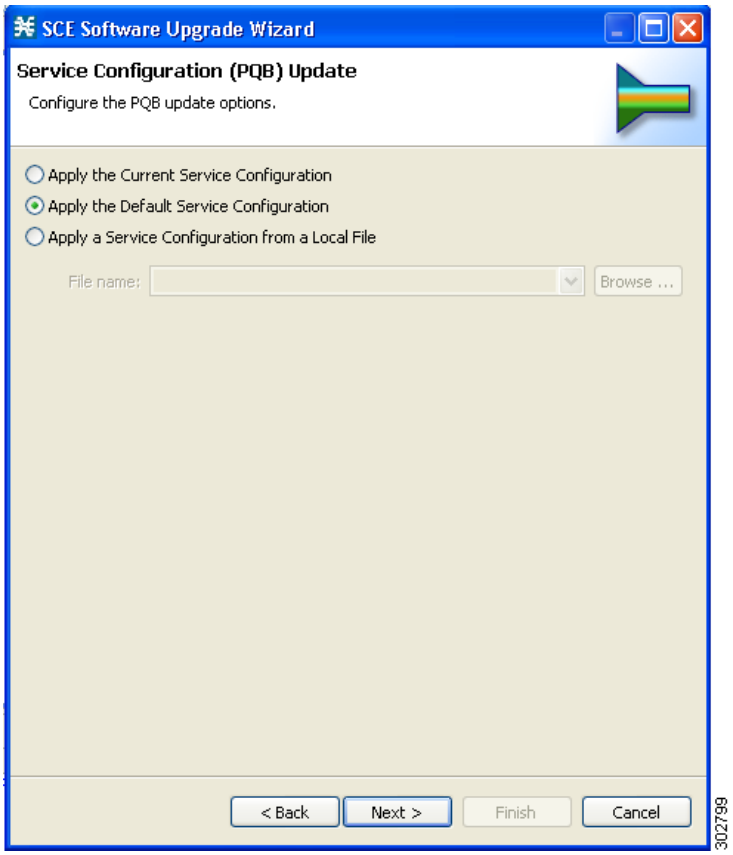
Note If you install the protocol pack during the upgrade, it must be the same version or a later version of the protocol pack you are upgrading from.

Figure 17 SCE Software Upgrade Wizard—Protocol Pack (SPQI) Update



Step 7 In the Service Configuration (PQB) Update pane (see Figure 18), check Apply the Default Service Configuration and click **Next**.

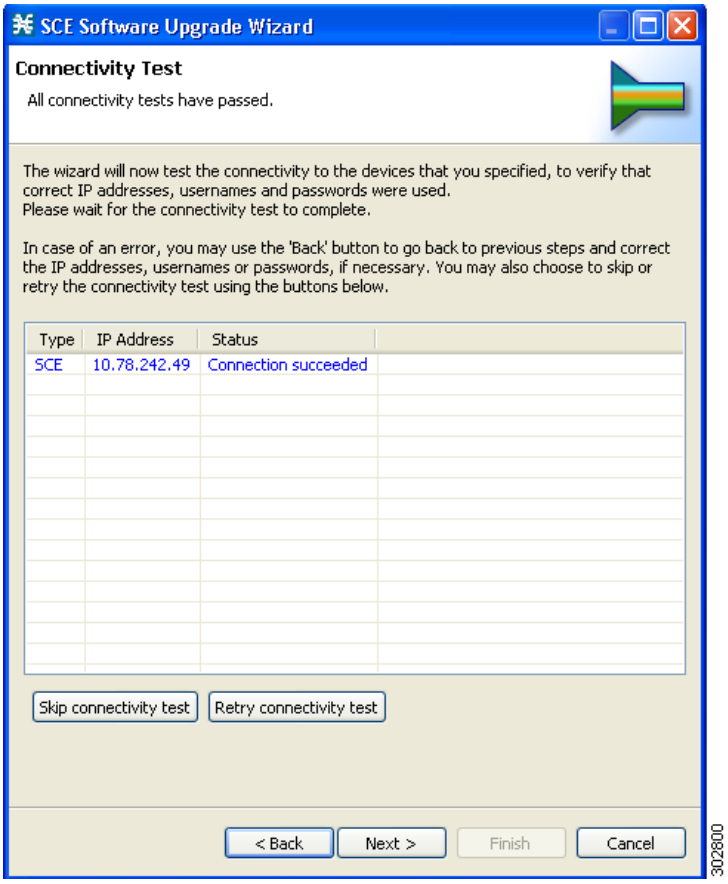
Figure 18 SCE Software Upgrade Wizard—Service Configuration (PQB) Update



Step 8 The Connectivity Test pane of the SCE Software Upgrade Wizard is displayed (see Figure 19). Click **Next**.

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

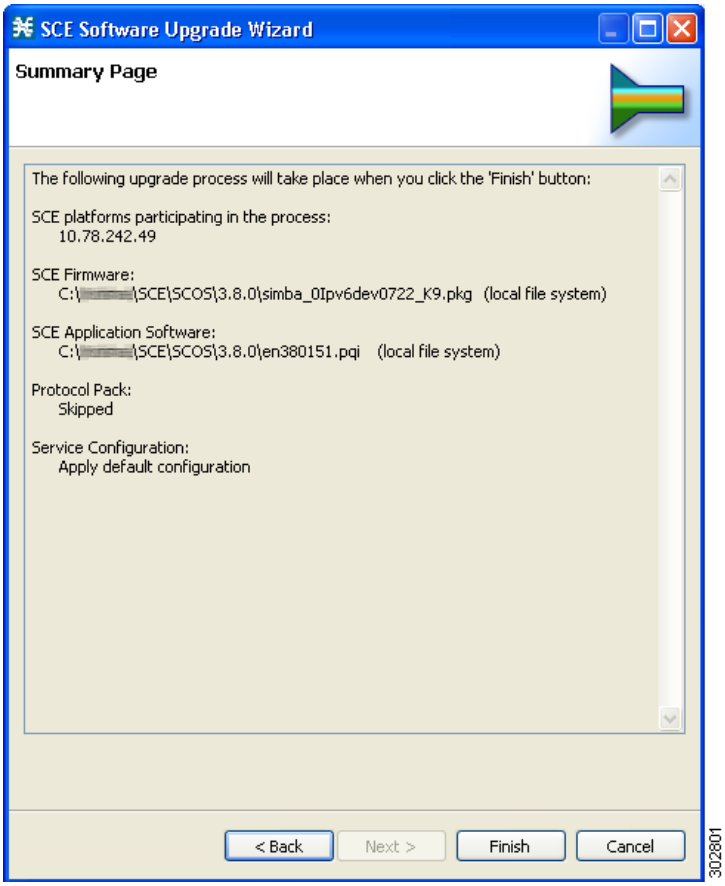
Figure 19 Connectivity Test



Step 9 The Summary pane summarizes all the information (see Figure 20). Verify that all the IP addresses and file locations are correct. In this pane, you can:

- Click **Back** to edit any information.
- Click **Finish** to begin the upgrade process as specified.

Figure 20 SCE Software Upgrade Wizard—Summary



4 Initial Configuration

This section describes the initial configuration of the system.

After all the Service Control components have been installed, perform these tasks to complete the initial setup and configuration of the system:

Step 1 Configure basic global parameters in the Cisco SCE platform, including these:

- Define the necessary IP addresses.
- Set the clock.
- Set the authorization-level passwords.
- Define RDR formatter destinations.

Step 2 Configure your site and a basic service configuration in the Cisco SCA BB Console. From the Network Navigator, run either the Usage Analysis wizard, the P2P Traffic Optimization wizard, or the P2P Traffic Optimization for Asymmetrical Routing wizard.

Step 3 From the Network Navigator, add the Subscriber Manager to the site.

Step 4 From the Network Navigator, configure a master password for the site.

Step 5 Configure the Subscriber Manager.

Note The initial setup process is flexible, and you may find that you prefer to do things slightly differently. The steps mentioned above can be considered as a suggested approach, rather than a mandatory approach.

Initial Configuration of the Cisco SCE 8000 Platform

Note The initial setup of the Cisco SCE 2000 platform should be performed by using the setup wizard. See the "Initial System Configuration" section on page 53 for more information about the Cisco SCE 2000 setup wizard.

There are several basic global parameters that must be correctly configured for the Cisco SCE platform to communicate properly with the outside world. The following is a brief summary of the initial setup parameters and commands. For more information, see the *Cisco SCE8000 10GBE Software Configuration Guide* or the *Cisco SCE8000 GBE Software Configuration Guide*.

- IP address and subnet mask of the Cisco SCE 8000 platform. This IP address is used by the GBE management interface.
- IP address of the default gateway.
- Hostname—The hostname is used to identify the Cisco SCE platform. It appears as part of the CLI prompt and is also returned as the value of the MIB-II object sysName.
  - The maximum length is 20 characters.
  - The default hostname is *SCE8000*.
- Passwords for user, admin, and root-level access. These are authorization-level passwords, not individual passwords. These passwords may be encrypted.

  These passwords must meet the following criteria:
  - Minimum length—Four characters
  - Maximum length—100 characters
  - Begin with an alpha character
  - Must contain only printable characters
- The default password for all levels is *cisco*.
- System clock—Current date and time. The clock and the calendar must always be synchronized.

- Time zone—The name or ID of the time zone along with the number of hours offset from Coordinated Universal Time (UTC).
- Domain name server—The default domain name used to complete unqualified host names, as well as up to three domain name servers, that are used for DNS lookup. You must also enable DNS lookup.
- RDR formatter destination—The Cisco SCE platform generates RDRs and sends them to the specified destinations (external collection systems) via the RDR formatter. You can configure up to eight RDR formatter destinations. Specify the IP address and port number for each destination.

Table 8 lists the commands both for displaying the currently configured values and for configuring these parameters. It also lists the command mode for each configuration command. All the **show** commands are executed in the user EXEC command mode.

Table 8 Initial Setup Configuration

Parameter	show Command	Configuration Command	Configuration Command Mode
Management IP address and subnet mask	**show interface GigabitEthernet 1/1 ip address**	**ip address** *x.x.x.x subnet-mask*	GigabitEthernet interface configuration
Default gateway	**show ip default-gateway**	**ip default-gateway** *x.x.x.x*	Global configuration
Hostname	**show hostname**	**hostname** *host-name*	Global configuration
Authorization-level passwords	—	**enable password level** *level [encryption-type] password*	Global configuration
Clock	**show clock** **show calendar**	**calendar set** *hh:mm:ss day month year* **clock read-calendar** or **clock set** *hh:mm:ss day month year* **clock update-calendar**	Privileged EXEC
Time zone	**show timezone**	**clock timezone** *zone-name offset-hours*	Global configuration
Domain name server	**show hosts**	ip domain-lookup **ip domain-name** *domain-name* **ip name-server** *server-address1 [server-address2] [server-address3]*	Global configuration
RDR formatter destination	**show rdr-formatter destination**	**rdr-formatter destination** *ip-address* **port** *port-number*	Global configuration

Initial Cisco SCA BB Configuration

Initial SCA BB configuration includes two main aspects:

- Defining your site—Defining all your Cisco Service Control components. Use the Usage Analysis wizard to define your site.
- Defining a basic service configuration.

Usage Analysis Wizard

Use this wizard to perform these tasks:

- Create the site.
- Create a service configuration called *Usage Analysis* with the following characteristics:
  - The mode is set to Report Only.
  - The maximum Transaction RDR rate is set as the default value (250) divided by the number of Cisco SCE devices.

- Configures the Reporter to produce these predefined reports:
  - Global Bandwidth per Service
  - Global Active Subscribers per Service
  - Top P2P Protocols
  - Global Hourly Call Minutes per Service (VoIP)

How to Use the Usage Analysis Wizard to Define the Default Site

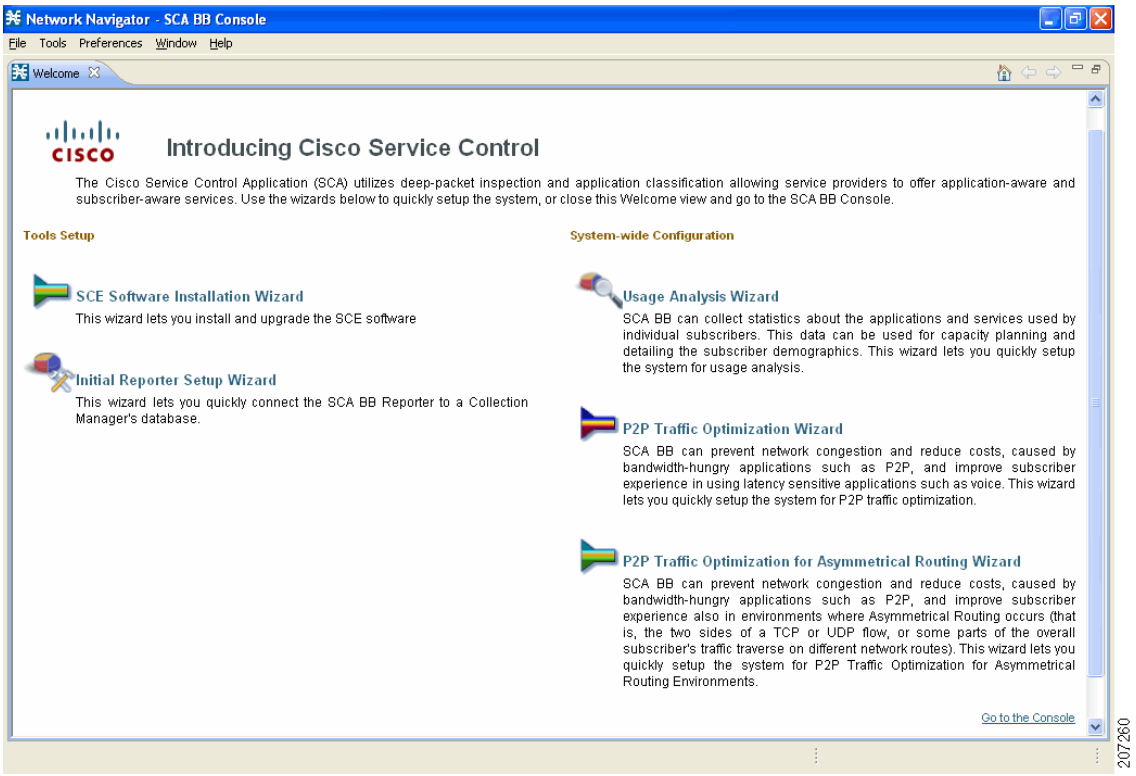
The Usage Analysis wizard allows you to create a simple model of devices and connect to them.

Note If they do not exist, the devices defined in the wizard are added to the default site in the Site Manager tree.

To use Usage Analysis Wizard to define the default site, complete these steps:

Step 1 From the Console main menu, choose **Help > Welcome.**
The Welcome window opens (see Figure 21).

Figure 21 Welcome Window

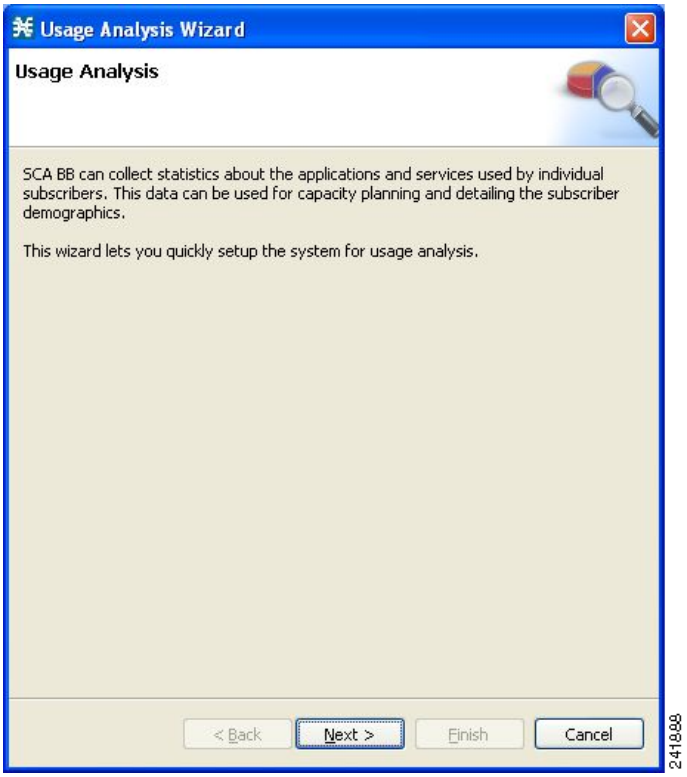


Step 2 Click **Usage Analysis Wizard.**

The Usage Analysis Wizard window appears (see Figure 22).

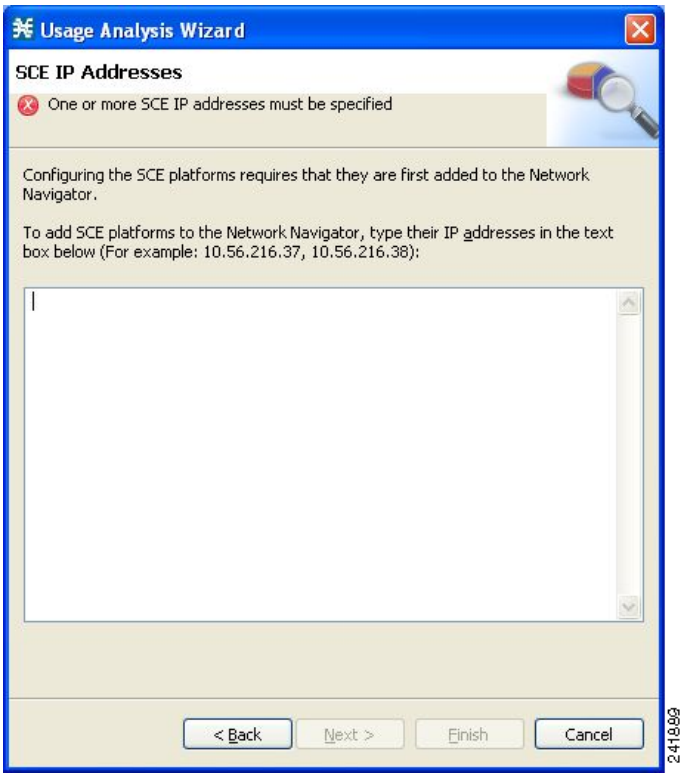
Step 3 Click **Next.**

Figure 22 Usage Analysis Wizard—Usage Analysis



The SCE IP Addresses window opens (Figure 23).

Figure 23 Usage Analysis Wizard—SCE IP Addresses Window



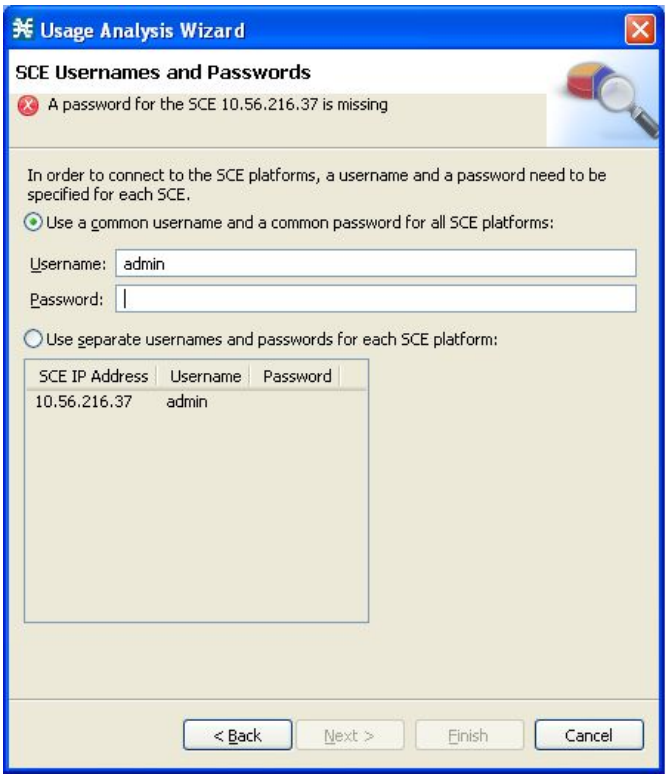
Step 4 In the text box, enter the IP addresses of the Cisco SCE devices that should be added to the model.

Note You can work with up to 20 Cisco SCE devices simultaneously by using the wizard.

Step 5 Click **Next.**

The SCE Usernames and Passwords window opens (see Figure 24).

Figure 24 Usage Analysis Wizard—SCE Usernames and Passwords Window



Step 6 Enter the user names and passwords for the SCE devices.

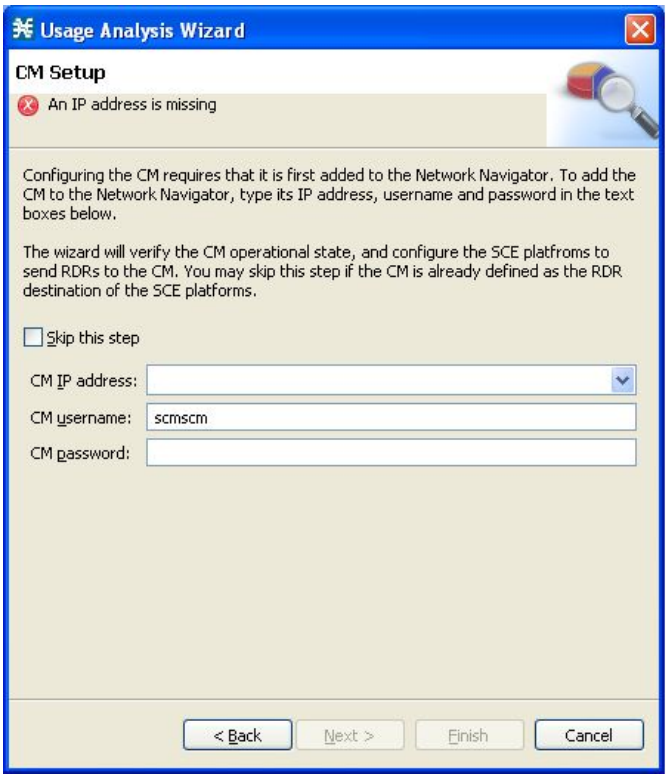
Do one of these:

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

Step 7 Click **Next.**

The CM Setup window opens (see Figure 25).

Figure 25 Usage Analysis Wizard—CM Setup Window



Step 8 Define the SCMS Collection Manager to use with this configuration.

Do one of these:

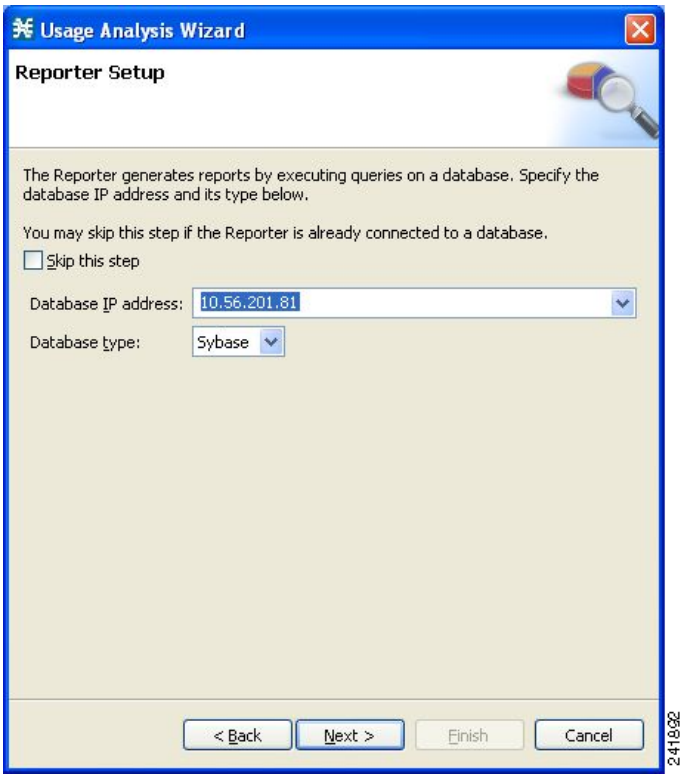
- Enter the IP address, user name, and password of the Collection Manager device in the appropriate fields.

  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.
- Check the **Skip this step** check box.

Step 9 Click **Next.**

The Reporter Setup window opens (see Figure 26).

Figure 26 Usage Analysis Wizard—Reporter Setup Window



Step 10 Define the database to which the Reporter tool should connect.

Do one of these:

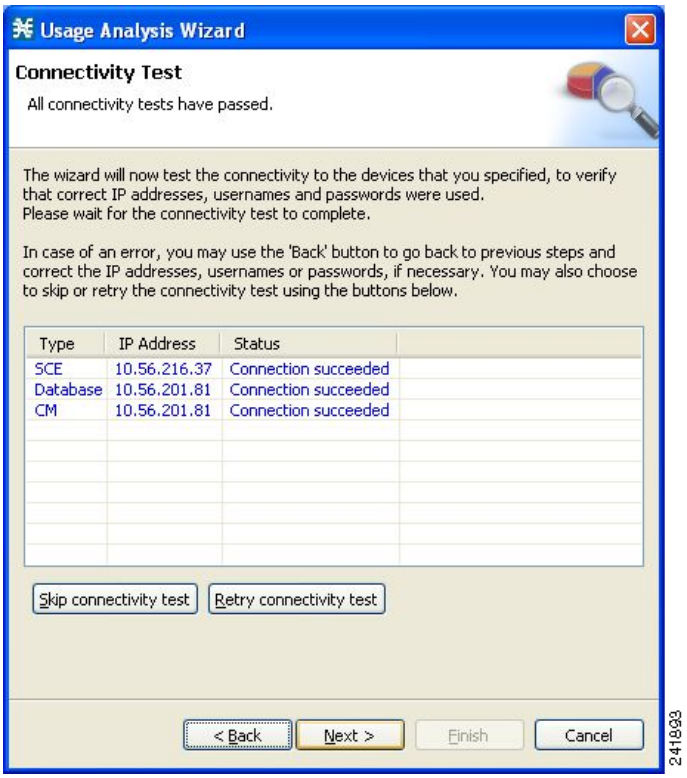
- Enter the IP address of the database and select the database type.

  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.
- Check the **Skip this step** check box.

Step 11 Click **Next.**

The Connectivity Test window opens (see Figure 27).

Figure 27 Usage Analysis Wizard—Connectivity Test Window



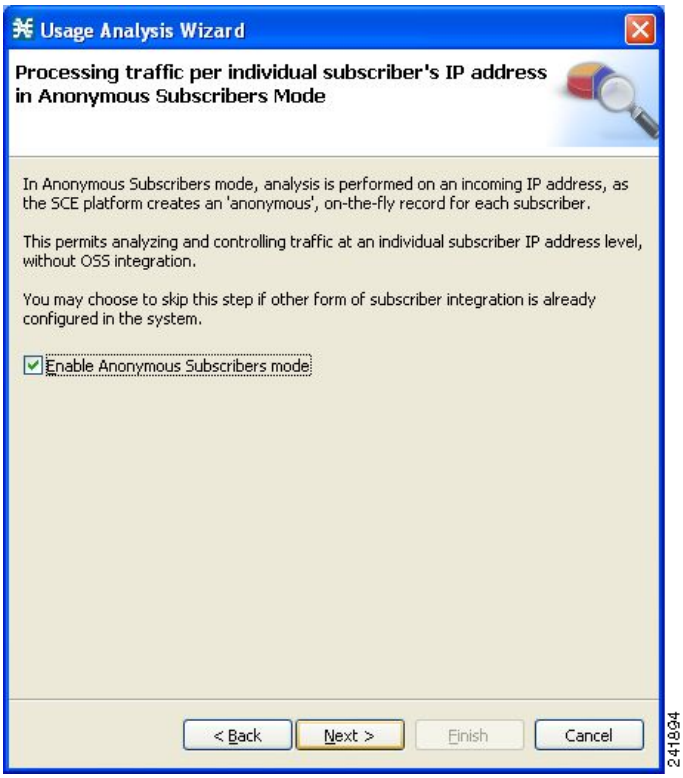
The wizard tests to see that the connections to the defined devices can be made.

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

Step 12 Click **Next.**

The Anonymous Subscribers window opens (see Figure 28).

Figure 28 Usage Analysis Wizard—Anonymous Subscribers Window

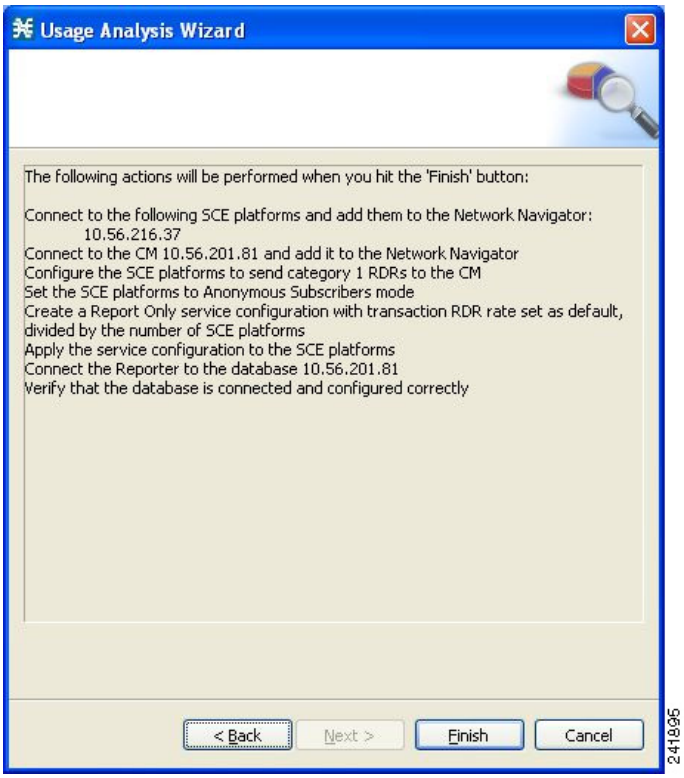


Step 13 To disable anonymous subscriber mode, uncheck the **Enable Anonymous Subscribers mode** check box.

Step 14 Click **Next.**

The Confirmation window opens (see Figure 29).

Figure 29 Usage Analysis Wizard—Confirmation Window

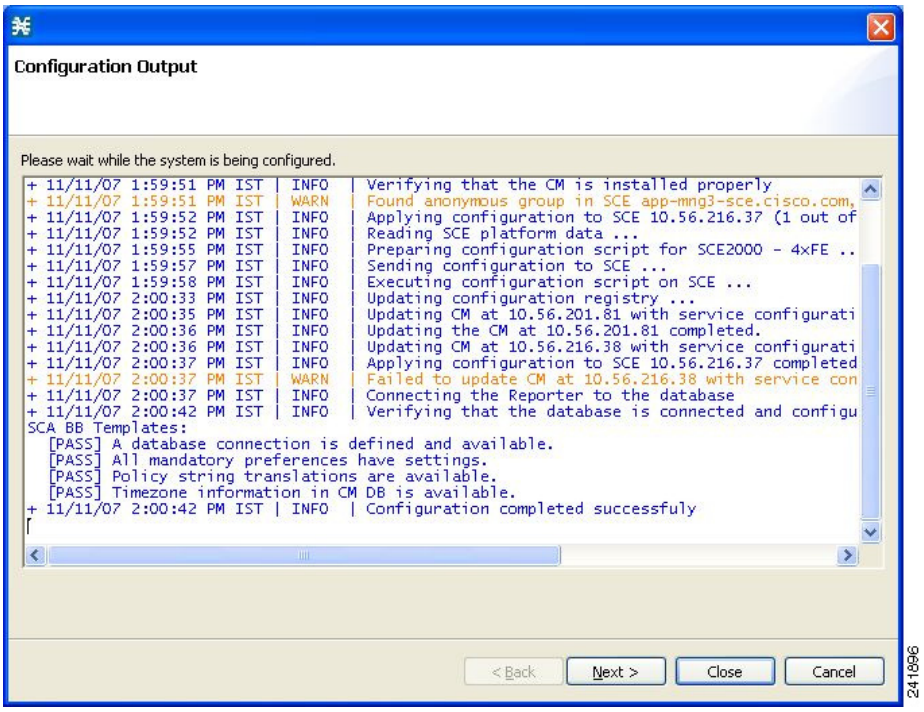


The actions that the wizard is about to take are listed on the page.

Step 15 Click **Finish.**

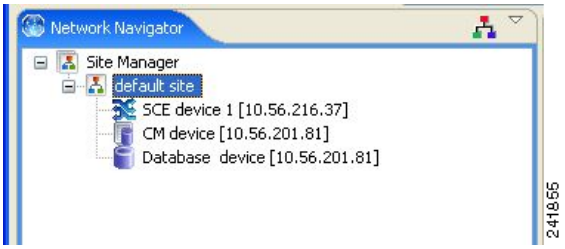
The Configuration Output window opens (see Figure 30).

Figure 30 Usage Analysis Wizard—Configuration Output Window



New devices are added to the default site of the Site Manager tree in the Network Navigator (see Figure 31).

Figure 31 Network Navigator



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

- The wizard cannot connect to any of the SCE devices that you listed in Step 4.
- You defined a Collection Manager in Step 8, but the wizard cannot connect to it.
- You defined a database in Step 10, but the wizard cannot connect to it.

If you defined a Collection Manager in Step 8, the SCE devices are configured so that the only category 1 RDR destination is the CM.

A new service configuration named Usage Analysis is created, and opens in the Service Configuration Editor (see Figure 32).

Figure 32 Service Configuration Editor

The service configuration has these characteristics:

- They are in Report Only mode.
- The maximum Transaction RDR rate is set as the default value (250) divided by the number of SCE devices. (To configure the Transaction RDR see How to Manage Transaction RDRs in the *Cisco Service Control Application for Broadband User Guide*. The content and structure of the Transaction RDR is listed in "Transaction RDR" in the "Raw Data Records: Formats and Field Contents" chapter of *Cisco Service Control Application for Broadband Reference Guide*.)

The service configuration is applied to the SCE devices.

If you defined a database in Step 10:

a. The SCA BB Reporter tool is connected to the selected database.

b. The first SCE platform entered in Step 4 is selected as the source of service configuration data.

c. The Next button is enabled.

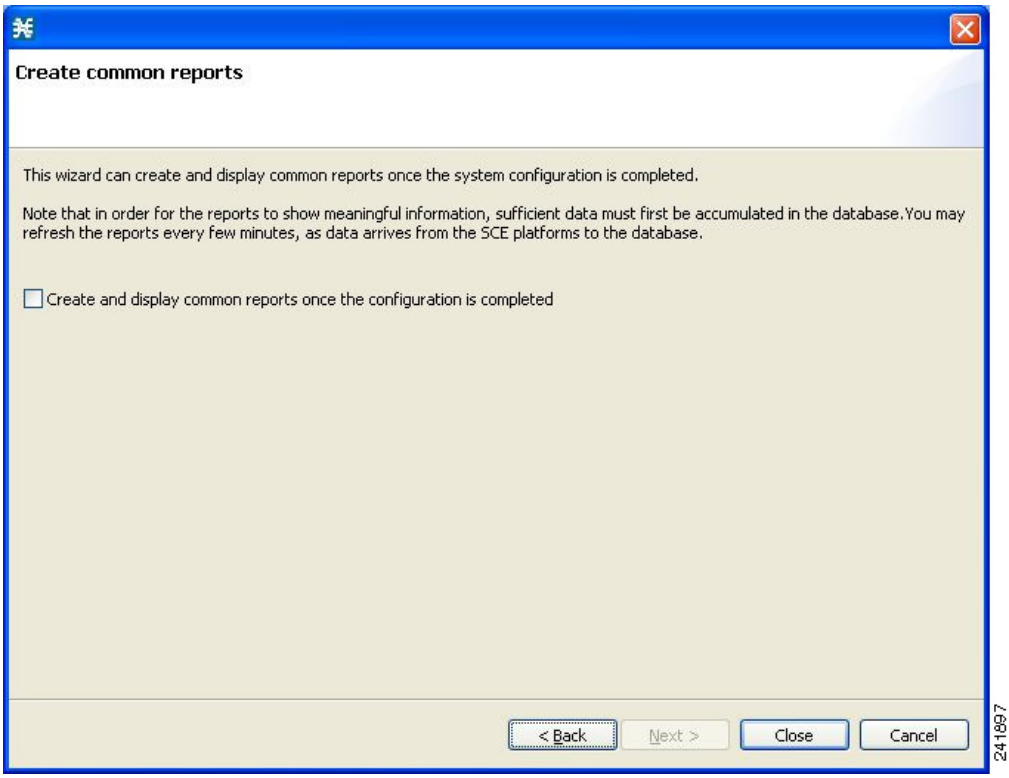
Step 16 If you did not define a database in Step 10, click **Close.**

The Usage Analysis wizard closes.

Step 17 Click **Next.**

The Create common reports window opens (see Figure 33).

Figure 33 Create Common Reports Window



Step 18 To create reports, check the **Create and display common reports once the configuration is completed** check box.

Note Report instances are created for four predefined report types:
- Global Bandwidth per Service
- Global Active Subscribers per Service
- Top P2P Protocols
- Global Hourly Call Minutes per Service (VoIP)

Step 19 Click **Close.**

The wizard closes.

The Reporter tool opens in the Console.

Report instances of each of the four report types open in the Report View of the Reporter tool.

Configuring the Subscriber Manager

After installing the SCMS Subscriber Manager, you can configure the Subscriber Manager to your specific needs. In particular, address these parameters:

- topology—Cluster or standalone
- introduction_mode—Pull or push
- support_ip_ranges—Whether IP ranges should be used in the installed setup

To configure the Subscriber Manager, edit the p3sm.cfg configuration file by using any standard text editor. The configuration file is described in detail in the Configuration and Management module and in the Configuration File Options module of *Cisco Service Control Management Suite Subscriber Manager User Guide*.

After you finish editing the **p3sm.cfg** configuration file, use the **p3sm** utility to update the Subscriber Manager with the new settings:

At your workstation shell prompt, run the **p3sm** command.

This **p3sm** command loads the configuration file and updates the Subscriber Manager configuration accordingly:

```
>p3sm --load-config
```

5 Cisco SCE 2000 Platform Installation

This chapter summarizes the topologies and installation of the Cisco SCE 2000 platform. In general, these installations and topologies are similar to that of Cisco SCE 8000 platform, but there are some differences.

Cisco SCE 2000 Platform Topologies

The Cisco SCE 2000 can be deployed in the same topologies as the Cisco SCE 8000 platform. Figure 34, Figure 35, Figure 36, Figure 37, and Figure 38 illustrate the Cisco SCE 2000 topologies.

Figure 34 Single SCE Platform Single Link: In-line Topology

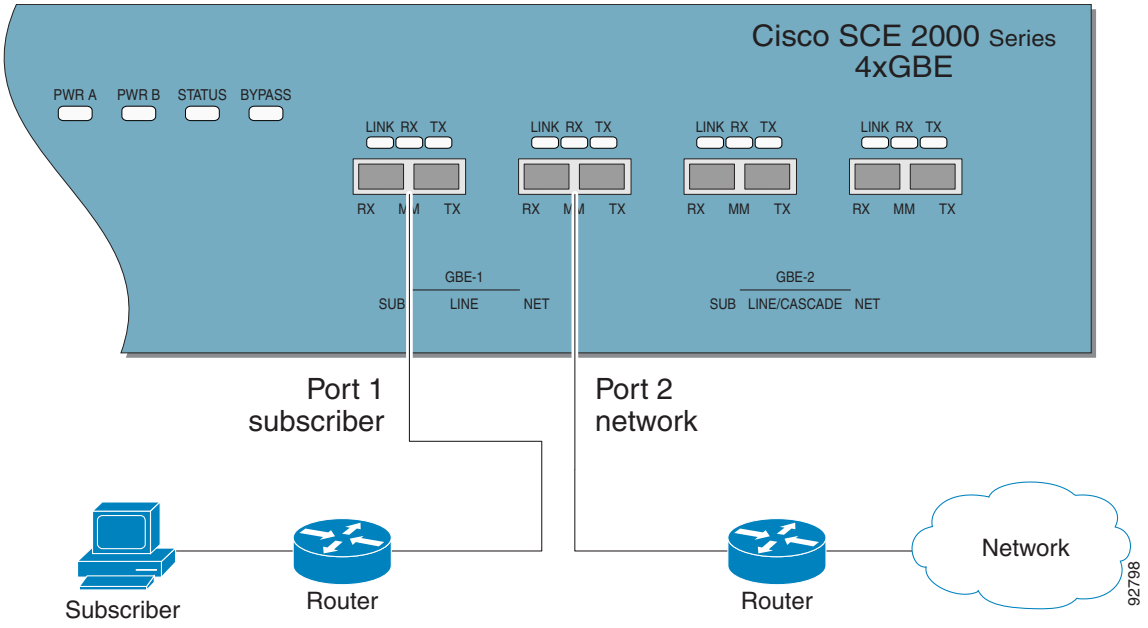


Figure 35 Single SCE Platform Dual Link In-line Topology

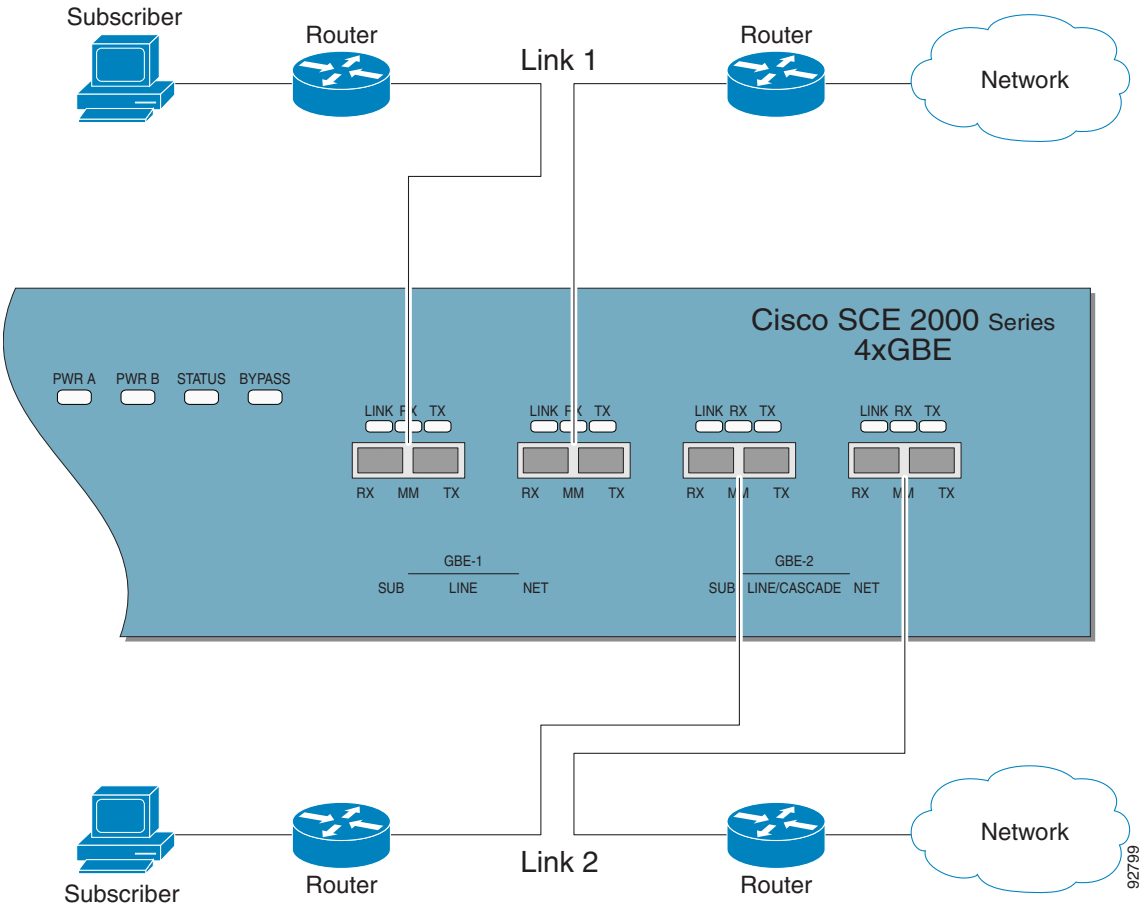


Figure 36 Single SCE Platform Single Link: Receive-Only Topology

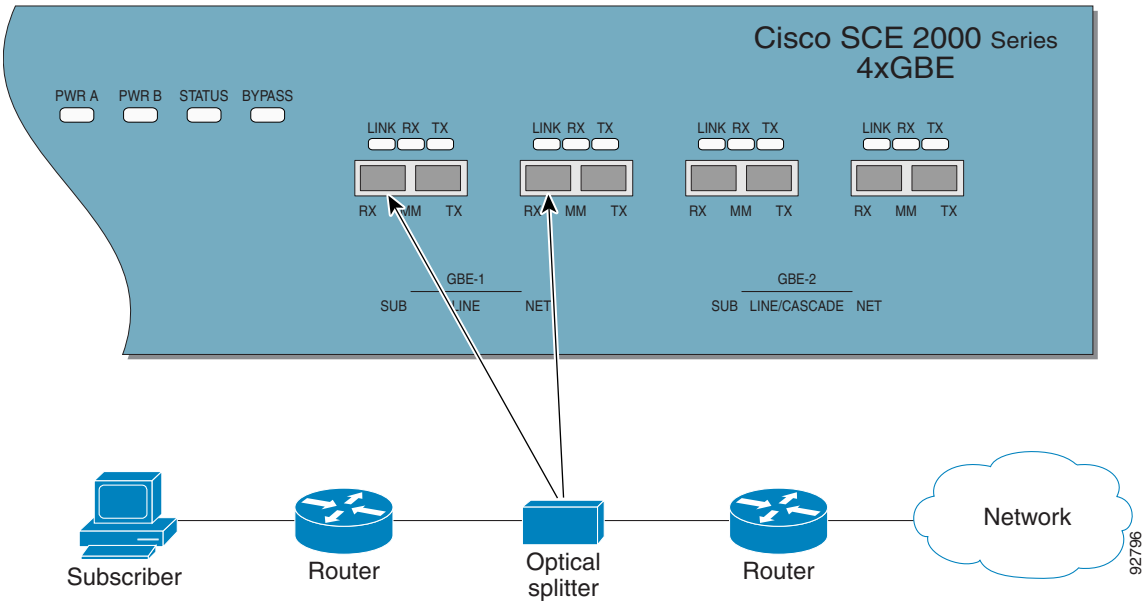


Figure 37 SCE Platform Dual Link: Receive-Only Topology

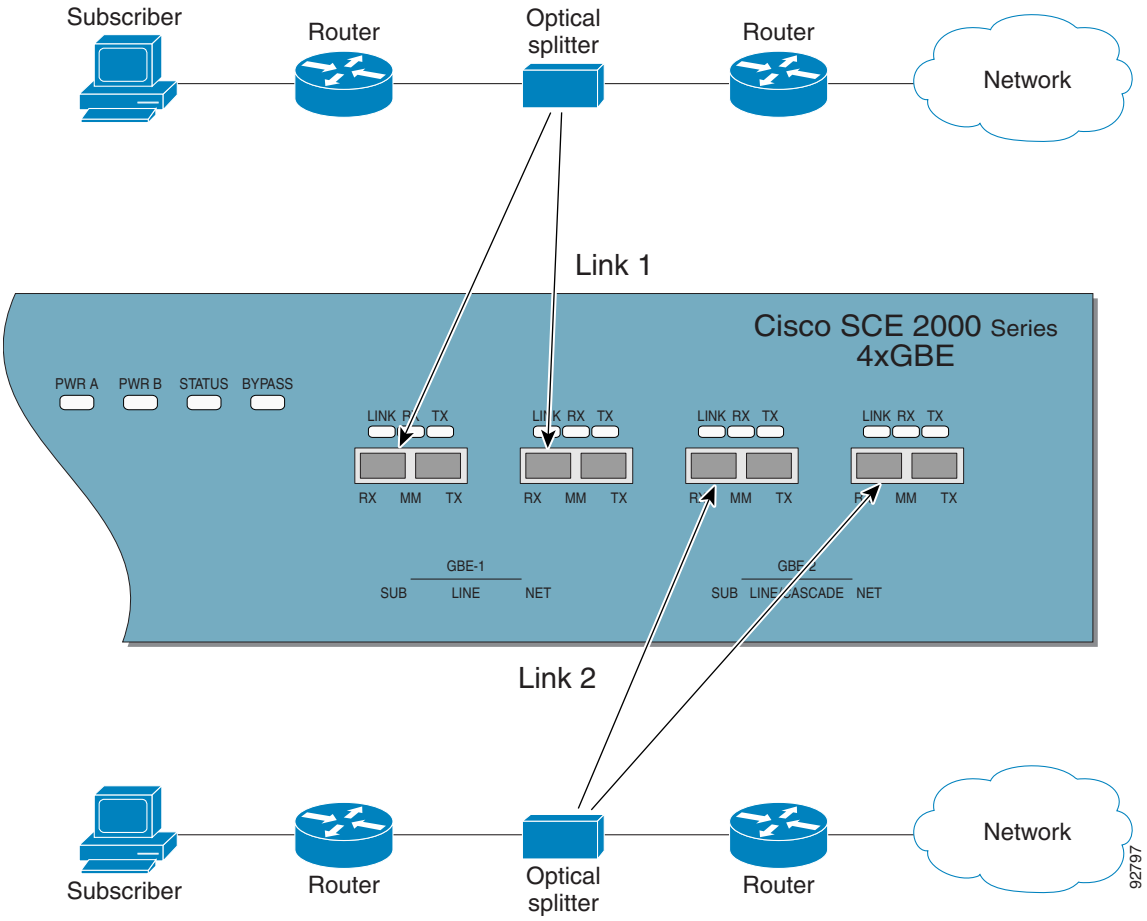
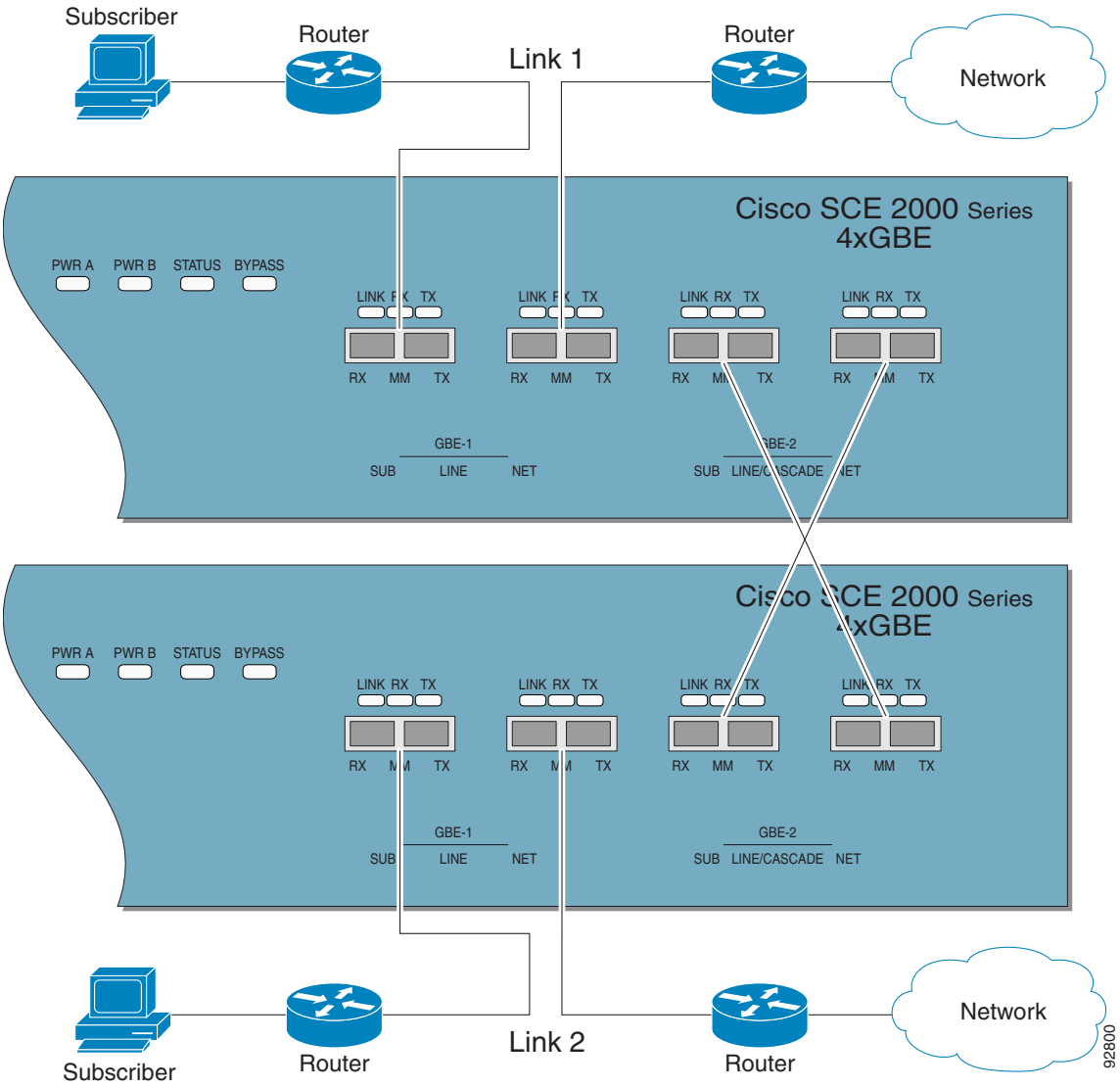


Figure 38 Two SCE Platforms: Dual Link In-line Topology



Installing a Cisco SCE 2000 Platform

To install the SCE platform, complete the following steps. (For more information, see the *Cisco SCE 2000 Installation and Configuration Guide*.)

Step 1 Install the SCE platform in the rack.

Step 2 Connect the chassis ground and the power.

Step 3 Connect the CON port to a local terminal and perform the initial configuration by using the setup wizard.

a. Press **Enter** several times until the Cisco logo appears on the local terminal and the setup configuration dialog is entered:

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' followed by 'Enter' for help.
Use ctrl-C to abort configuration dialog at any prompt.
Use ctrl-Z to jump to the end of the configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to continue with the System Configuration Dialog? [yes/no]: y
```

b. Type **y** and press **Enter**.

The system configuration dialog begins. See the "Initial System Configuration" section on page 53 for information about the setup wizard.

Step 4 Connect the MNG port to the local LAN.

If you are using both MNG ports for redundancy, connect them to the LAN via a switch.

Step 5 Cable the line ports. (See the "SCE 2000 Connectivity" section on page 55 for a summary of proper cabling for various topologies.)

Initial System Configuration

Upon initial connection to the local terminal, the system configuration wizard automatically runs to guide the user through the entire setup process. The wizard prompts for all necessary parameters, displaying default values, where applicable. You may accept the default values or define other values.

Except for the time settings, which take effect immediately when entered, the new configuration is applied and saved only at the end of the dialog when approved by the user. Therefore, if the setup dialog is aborted, no change takes place in the configuration, other than time settings (if entered).

When the dialog is complete, you may review the new configuration before applying it. The system displays the configuration, including parameters that were not changed. The system also displays any errors that are detected in the configuration. When the configuration is satisfactory, you may apply and save the new configuration.

Table 9 lists all the parameters included in the initial configuration. We recommend that you obtain values for any parameters that you configure at this time before beginning the setup.

Note For further information about any configuration step or specific parameter, see the relevant section of *Cisco SCE 2000 and SCE 1000 Software Configuration Guide*.

Setup Command Parameters

Table 9 Setup Command Parameters

Parameter	Definition
IP address	IP address of the SCE 2000.
subnet mask	Subnet mask of the SCE 2000.
default gateway	Default gateway.
Hostname	Character string used to identify the SCE 2000. Maximum 20 characters.
admin password	Admin-level password. Character string containing 4 to 100 characters beginning with an alpha character.
root password	Root-level password. Character string containing 4 to 100 characters beginning with an alpha character.
password encryption status	Enable or disable password encryption.
Time Settings	

Table 9 Setup Command Parameters (continued)

Parameter	Definition
time zone name and offset	Standard time zone abbreviation and minutes offset from UTC.
local time and date	Current local time and date. Use the 00:00:00 1 January 2002 format.
SNTP Configuration	
broadcast client status	Set the status of the SNTP broadcast client. If enabled, the SCE synchronizes its local time with updates received from SNTP broadcast servers.
unicast query interval	Interval in seconds between unicast requests for update. The range is from 64 to 1024.
unicast server IP address	IP address of the SNTP unicast server.
DNS Configuration	
DNS lookup status	Enable or disable IP DNS-based hostname translation.
default domain name	Default domain name to be used for completing unqualified host names.
IP address	IP address of domain name server (maximum of three servers).
RDR Formatter Destination Configuration	
IP address	IP address of the RDR-formatter destination.
TCP port number	TCP port number of the RDR-formatter destination.
Access Control Lists	
Access Control List number	Number of ACLs required. IP addresses permitted and denied access for each management interface. You may want ACLs for these: • Any IP access • Telnet access • SNMP GET access • SNMP SET access
list entries (maximum 20 per list)	IP address, and whether permitted or denied access.
IP access ACL	ID number of the ACL controlling IP access.
telnet ACL	ID number of the ACL controlling telnet access.
SNMP Configuration	
SNMP agent status	Enable or disable SNMP management.
GET community names	Community strings to allow GET access and associated ACLs (maximum 20).
SET community names	Community strings to allow SET access and associated ACLs (maximum 20).
trap managers (maximum 20)	Trap manager IP address, community string, and SNMP version.
Authentication Failure trap status	Sets the status of the Authentication Failure traps.
enterprise traps status	Sets the status of the enterprise traps.
system administrator	Name of the system administrator.
Topology Configuration	
Connection mode	Is the SCE 2000 installed using inline topology or receive-only topology using an optical splitter?
type of deployment	Is this a cascade topology, with two SCE 2000s connected via the cascade ports? Or is this a single platform topology?

Table 9 Setup Command Parameters (continued)

Parameter	Definition
physically connected link (cascade topology only)	In a cascade deployment, this parameter sets the index for the link that this SCE 2000 is deployed on. The options for SCE 2000 are link-0 or link-1. In a single SCE 2000 platform deployment, this parameter is not relevant since one SCE 2000 is deployed on both links. In this case, the link connected to port1-port2 is by default link-0 and the link connected to port3-port4 is by default link-1.
priority (cascade topology only)	Is this SCE 2000 the primary or secondary SCE 2000.
on-failure behavior (inline connection mode only)	Is the failure behavior be bypass or cutoff of the link.
Admin status of the SCE 2000 after abnormal boot	After a reboot due to a failure, should the SCE 2000 remain in a Failure status or move to operational status provided no other problem was detected?

SCE 2000 Connectivity

Table 10, Table 11, Table 12, Table 13, and Table 14 summarize SCE 2000 connectivity for the basic topologies.

Receive-only topologies use only Receive fibers.

Note Receive-only topologies can be implemented using either an optical splitter or a switch. If a switch is used, it must support SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN-ports destinations.

Table 10 Single Link Inline Connectivity

GBE Port	Link	Side
0/1	Link 0	Subscribers
0/2	Link 0	Network

Table 11 Dual Link Inline Connectivity

GBE Port	Link	Side
0/1	Link 0	Subscribers
0/2	Link 0	Network
0/3	Link 1	Subscribers
0/4	Link 1	Network

Table 12 Cascade Connectivity

This port on SCE 2000 #1	Connects to this...
0/1	Subscriber-side network element
0/2	Network-side network element
0/3 (cascade port)	Port 0/4 on SCE 2000 #2
0/4 (cascade port)	Port 0/3 on SCE 2000 #2
This port on SCE 2000 #2	**Connects to this....**

Table 12 Cascade Connectivity (continued)

This port on SCE 2000 #1	Connects to this...
0/1	Subscriber-side network element
0/2	Network-side network element
0/3 (cascade port)	Port 0/4 on SCE 2000 #1
0/4 (cascade port)	Port 0/3 on SCE 2000 #1

Table 13 External Optical Bypass Module Connectivity: Single Link

This Optical Bypass Component	Connects to this...
Sub port	Subscriber-side network element
Net port	Network-side network element
Sub fiber of the pigtail fiber	Sub port of the GBE-1 Line ports on the SCE 2000
Net fiber of the pigtail fiber	Net port of the GBE-1 Line ports on the SCE 2000
Control port	**Bypass 1** 9-pin D-Type connector on the rear panel of the SCE 2000 platform

Table 14 External Optical Bypass Module Connectivity: Dual Link

External Optical Bypass Module #1	
This Optical Bypass Component	**Connects to this...**
Sub port	Subscriber-side network element
Net port	Network-side network element
Sub fiber of the pigtail fiber	Sub port of the GBE-1 Line ports on the SCE 2000
Net fiber of the pigtail fiber	Net port of the GBE-1 Line ports on the SCE 2000
Control port	Bypass 1 9-pin D-Type connector on the rear panel of the SCE 2000 platform
External Optical Bypass Module #2	
This Optical Bypass Component	**Connects to this...**
Sub port	Subscriber-side network element
Net port	Network-side network element
Sub fiber of the pigtail fiber	Sub port of the GBE-2 Line/Cascade ports on the SCE 2000
Net fiber of the pigtail fiber	Net port of the GBE-2 Line/ Cascade ports on the SCE 2000
Control port	Bypass 2 9-pin D-Type connector on the rear panel of the SCE 2000 platform

MGSCP Topologies

In an MGSCP deployment, the exact cabling scheme depends on the number and arrangement of ports in the EtherChannel in the Cisco 7600 Series router. It is, therefore, not possible to give exact cabling schemes. See the following general guidelines when designing the cabling scheme:

- Because there are two links per Cisco SCE 2000 platform, the minimum number of platforms required is half the number of links used.
- Each link corresponds to one port on the EtherChannel on the Cisco 7600 Series router. Each EtherChannel supports a maximum of eight ports. Therefore, if all eight EtherChannel ports are configured, four Cisco SCE 2000 platforms are required.

- For N+1 redundancy, two ports (connected to the standby platform) must be configured as standby ports on both ECs.
  - For N+1 redundancy, one router and five Cisco SCE 2000 platforms would be used to support eight links.
- If two Cisco 7600 Series routers are used (for network redundancy), one link on each Cisco SCE 2000 platform is connected to each router. This topology requires twice the number of Cisco SCE 2000 platforms, one platform for each link.
  - Minimum of eight Cisco SCE 2000 platforms are required to support eight ports.
  - For N+1 redundancy, nine Cisco SCE 2000 platforms would be used to support eight active links.

When cabling to the EC, follow these guidelines:

- Cisco SCE platform ports *must* be connected to the EtherChannel ports in the same order on both sides.
- EtherChannel ports *must* be sorted in an ascending order by their physical interface numbers.
- In a topology with two Cisco 7600 Series routers, the order of connection to the EtherChannel ports must be the same on both routers. For both routers to send the traffic of a given subscriber to the same SCE platform, the SCE platforms must be connected to both routers in the same order (one SCE platform connected to the first link on both routers, another SCE platform connected to the second link on both routers, and so on).

6 System Requirements and Prerequisites

This chapter summarizes the system requirements and prerequisites of the Cisco SCE 2000 platform.

Overall System Requirements

- The SCE platform—Local console or management workstation connected to LAN.
- Cisco SCA BB—Workstation running Windows 2000, Windows XP, Windows Vista, or Windows 7.
- SCMS Subscriber Manager—Either of these:
  - Solaris—Sun SPARC machine (64 bit) running 64-bit versions of Solaris 9 or Solaris 10 with a 64-bit version of the Java Virtual Machine.
  - Linux—Intel-based machine with a 32-bit or 64-bit CPU running a 32-bit version of Linux with a 32-bit version of the Java Virtual Machine.

  The actual number of computers required depends on the number of subscribers in the system.
- SCMS Collection Manager—either of these:
  - Solaris—Sun SPARC machine running Solaris 8 or Solaris 9.
  - Linux Red Hat—IA32 machine running Red Hat Enterprise Linux 3.0 or Red Hat Enterprise Linux 4.0.

  The actual number of computers required depends on the amount of traffic in the system.
- SCA Reporter—Workstation running Windows 2000, Windows XP, Windows Vista, or Windows 7.

SCA BB System Requirements

These sections describe the SCA BB system requirements:

- Hardware Requirements, page 58
- Operating System Requirements, page 58
- Java Runtime Environment, page 58

Hardware Requirements

The hardware requirements are:

- At least 1024 MB RAM is required to run the Console.
- Minimal supported screen resolution for the Console is 1024 x 768 pixels.

Operating System Requirements

The Cisco SCA BB Console can run on Windows 2000, Windows XP, Windows Vista, or Windows 7.

Java Runtime Environment

If you are using the optional SCA BB Service Configuration Utility, servconf, it requires access to JRE version 1.6.

You can download a JRE from the Sun™ website at http://java.com/en/download/.

To verify that the JRE is installed, run **java-version** at the command prompt. The Java version should start with 1.6.

If a different version of JRE is also installed on the workstation, you may need to tell **servconf** where to find the appropriate JRE. Do this configuration by setting the JAVA_HOME environment variable to point to the JRE 1.6 installation directory. For example:

```
JAVA_HOME=C:\Program Files\Java\j2re1.6_08
```

Subscriber Manager System Requirements

You can install the SCMS Subscriber Manager on these platforms:

- Solaris—Sun SPARC machine (64-bit) running 64-bit versions of Solaris 9 or Solaris 10 with a 64-bit version of the Java Virtual Machine. See Table 15 and Table 16.
- Linux—Intel-based machine with a 32-bit or 64-bit CPU running a 32-bit version of Linux with a 32-bit version of the Java Virtual Machine. See Table 15 and Table 17.

The machine should conform to the system requirements listed in Table 15, Table 16, and Table 17.

Note The specifications listed in Table 15 are minimal. Verify the specifications to guarantee specific performance and capacity requirements.

Table 15 Minimal System Hardware Requirements

Item	Requirement
CPU	The CPU requirements are: • Sun SPARC, 64 bit, minimum 500 MHz (for Solaris) • Intel processor, 32 or 64 bit, minimum 1 GHz (for Linux Red Hat)
RAM	Minimum 1 GB
Free Disk Space	Minimum 3 GB total, of which: • Minimum 1 GB free on partition where VARDIR (SM database repository) is installed • Minimum 0.5 GB free on partition where PCUBEDIR (Subscriber Manager files) is installed • Minimum 200 MB free on partition where /tmp is mounted
Network Interface	Depends on whether the configuration includes a cluster: • Without cluster—One (1) 100BASE-T Ethernet • With cluster—Six (6) 100BASE-T Ethernet
CD-ROM drive	Recommended

For the hardware and software system requirements for the Veritas Cluster Server, see the Veritas Cluster Server chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Table 16 Solaris System Software Requirements

Item	Requirement
OS	Solaris 5.9 64 bit or later; currently, only 64-bit versions of Solaris 5.9 and 5.10 are supported. Solaris Core Installation.
System Packages	Mandatory: • SUNWbash—GNU Bourne-Again shell (bash). • SUNWgzip—GNU Zip (gzip) compression utility. • SUNWzip—Info-Zip (zip) compression utility. • SUNWlibC—Sun Workshop Compilers Bundled libC. • SUNWlibCx—Sun WorkShop Bundled 64-bit libC. • sudo (superuser do) package. Optional: • SUNWadmap—System administration applications. • SUNWadmc—System administration core libraries.

Note We recommend to apply the latest patches from Sun. You can download the latest patches from the Sun patches website.

Table 17 Red Hat System Software Requirements

Item	Requirement
OS	Red Hat Enterprise Linux AS/ES 4.0/5.0; currently, both 32-bit and 64-bit versions are supported. Red Hat Core Installation.
System Packages	Mandatory: • GNU Bourne-Again shell (bash-2.05b-29.i386.rpm). • GNU Data Compression Program (gzip-1.3.3-9.i386.rpm). • File compression and packaging utility (zip-2.3-16.i386.rpm). • Standard C++ libraries for Red Hat Linux 6.2 backward compatibility (compat-gcc-7.3-2.96.122.i386.rpm). • sudo (superuser do) package. For integrating with the C API: • GNU cc and gcc C compilers (gcc-3.2.3-20.i386.rpm). • C++ support for the GNU gcc compiler (gcc-3.2.3-20.i386.rpm).

Note We recommend that you apply the latest patches from Red Hat.

Note Only 32-bit versions of Linux are supported, but it is possible to install 32-bit Linux on a 64-bit CPU.

Cisco Service Control Collection Manager System Requirements

The Cisco Service Control Collection Manager and its database are software components that run on a server platform. They can be installed on any of these configurations:

- Sun SPARC machine (64 bit) running 64-bit versions of Solaris 9 or Solaris 10. (See the "Solaris Requirements" section on page 62)
- Intel machine (32 bit or 64 bit) running 32-bit versions of Red Hat Enterprise Linux 3.0 or Red Hat Enterprise Linux 4.0. (See the "Red Hat Linux Requirements" section on page 64)

All configurations use a 32-bit Java Virtual Machine (JVM).

Note The Collection Manager must run on its own machine. You cannot run the Collection Manager on the same machine as the Subscriber Manager and other applications.

Note When using the bundled Sybase database, the server on which you install the Collection Manager can have a maximum of four CPU cores.

These sections describe the Collection Manager system requirements:

Checking a System's Prerequisites

The CM distribution contains a script, check_prerequisites.sh, located in the install_scripts directory:

check_prerequisites.sh [**--sybhome=***SYBHOME*] [**--cmhome=***CMHOME*] [**--datadir=***DATADIR*]

The script helps to determine if a system meets the requirements for installing a CM or the bundled Sybase database. It also checks the overall readiness of the system for a Collection Manager or Sybase installation. The main prerequisites that are checked are:

- CPU speed
- Amount of RAM
- OS version (Solaris 9 or 10, Red Hat Enterprise Linux 4 or 5)
- Additional required and optional packages
- Python installed and executable in path
- Free space for CM and Sybase homes
- Names for all the network interface cards (NICs)
- Sybase kernel parameters
- Locale and time zone formats

Table 18 describes the options available in the check_prerequisites.sh script.

Table 18 check_prerequisites.sh Script Options

Script Options	Descriptions
--sybhome=*SYBHOME*	Intended home directory for Sybase installation.
--cmhome=*CMHOME*	Intended home directory for CM installation.
--datadir=*DATADIR*	Intended data directory for Sybase data files (for the Datadir installation method). This directory should be created on a different mount, and not on the CM mount.

Note All the directories listed in Table 18 must be created before running the check_prerequisites.sh script.

Solaris Requirements

Collection Manager Release 3.7.0 or later can be installed on any Oracle SPARC machine running Solaris that conforms to the requirements listed in these sections:

- Hardware, page 62
- Software and Environment, page 62
- Setting the Locale and Time Zone, page 63

Hardware

The Collection Manager's hardware requirements are:

- Minimum 500 MHz CPU
- Minimum 1 GB RAM per CPU
- Hard disk:
  - One hard disk, at least 18 GB
  - (Recommended for bundled installations) A second hard disk (at least 18 GB), to store Sybase data
- 100BASE-T network interface

Software and Environment

The Collection Manager's software and environment requirements are:

- Solaris Version 5.9 64-bit build 04/01 or later (Currently, only Solaris Version 5.9 and 5.10 are supported.)
- Solaris Core Installation
- Install these additional packages:

system	SUNWbash	GNU Bourne-Again shell (bash)
system	SUNWgzip	GNU Zip (gzip) compression utility
system	SUNWzip	Info-Zip (zip) compression utility
system	SUNWlibC	Sun Workshop Compilers Bundled libC
system	SUNWlibCx	Sun WorkShop Bundled 64-bit libC

- If you are installing the CM in a bundled mode with the Sybase database, you must install this package:

system	SUNWipc	Interprocess Communication

- (Optional) The following packages can also be installed (for sysadmin applications such as sys-unconfig), if required:

system	SUNWadmap	System administration applications
system	SUNWadmc	System administration core libraries

- To use the Python scripts, a Python Interpreter Version 2.2.1 or later must be present in the system. You can install these Interpreter package:

application	SMCpythn (Solaris 9) SMCpython (Solaris 10)	Python

- The Python package requires the installation of two additional packages:

application	SMClibgcc	libgcc
application	SMCncurs	ncurses

- You can download the above mentioned packages from http://sunfreeware.com

  The root (/) partition must have at least 104 MB of free space to install these packages.
- Apply the latest recommended patches from Sun:
  - For Solaris 9, go to http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/xos-9&nav=pub-patches.
  - For Solaris 10, go to http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/xos-10&nav=pub-patches.
  - For Java, go to http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE.
- If you are using Sybase, install the current Solaris patches recommended by Sybase:
- At least 8 GB free space on the partition in which the CM is to be installed. (This space is used for CSV storage and persistent buffers.)
- (For installations with bundled Sybase) At least 3 GB free space on one partition for the Sybase home directory.
- (For installations with bundled Sybase) Free space on one partition to hold the desired size of the Sybase data and logs (the sizes are configurable at installation time).
- (For installations with bundled Sybase where the legacy [pre-3.0] Cisco Service Control Reporter is to be used.) An FTP server should be listening on port 21 so that the Cisco SCA Reporter can authenticate against it.
- (For installations with bundled Sybase) Before installation, verify that all the IP addresses that are configured for the machine NICs have hostnames associated with them in /etc/hosts or in another active naming service. (This is a limitation of Sybase Adaptive Server Enterprise.)
- (For installations with bundled Sybase) Use the set_shmmax.sh script (located in install-scripts/) to configure the kernel memory.
- Additionally, at startup, load the IPC module by adding these lines in the /etc/system file:

  ```
  forceload: sys/shmsys
  ```

- If you are using database periodic delete, the scmscm user should be able to schedule and run cron jobs.

Setting the Locale and Time Zone

For correct CM and Sybase operation, U.S. English locale must be used. To set the locale, add this line in the /etc/TIMEZONE configuration file (changes to this file require a restart to take effect):

```
LANG=en_US
```

Solaris also requires this locale to be installed. Verify that the locale is installed by checking whether the directory /usr/lib/locale/en_US exists. If the directory does not exist, install the locale files from the Solaris CDs.

Red Hat Linux Requirements

Collection Manager Version 3.7.0 or later can be installed on any i386 running Red Hat Linux that conforms to the requirements listed in these sections:

- Hardware, page 64
- Software and Environment, page 64
- Setting the Locale and Time Zone, page 64

Hardware

The hardware requirements are:

- Minimum 800 MHz CPU
- Minimum 1 GB RAM per CPU
- Hard disk:
  - One hard disk, at least 18 GB
  - (Recommended for bundled installations) A second hard disk (at least 18 GB), to store Sybase data
- 100BASE-T network interface

Software and Environment

The software and environment requirements are:

- Red Hat Linux 4.0:
  - kernel-2.6.9-5
  - glibc-2.3.4-2
  - compat-libstdc++-33-3.2.3-47.3
- Red Hat Linux 5.0:
  - kernel-2.6.18-8.el5
  - glibc-2.5-12
  - compat-libstdc++-33-3.2-61
- Red Hat Enterprise Base Installation.
- (For installations with bundled Sybase) Install the additional package compat-libstdc++. This package is available on the Red Hat installation CD.
- Apply the latest recommended patches from Red Hat.
- (For installations with bundled Sybase) Install current patches recommended by Sybase.
- Reserve at least 8 GB free on the partition where the Collection Manager is to be installed. (This is used for CSV storage and persistent buffers.)
- (For installations with bundled Sybase) At least 1 GB free on some partition for the Sybase home directory.
- (For installations with bundled Sybase where the legacy (pre-Version 3.0) Cisco Service Control Application Suite Reporter is to be used.) An FTP server should be listening on port 21 so that the SCA Reporter can authenticate against it.
- (For installations with bundled Sybase) Before installation, verify that all IP addresses that are configured for the machine NICs have hostnames associated with them in /etc/hosts or in another active naming service. (This is a limitation of Sybase Adaptive Server Enterprise.)
- (For installations with bundled Sybase) Use the set_shmmax.sh script (located in install-scripts/) to configure the kernel memory.
- If you are using database periodic delete, the scmscm user should be able to schedule and run cron jobs.

Setting the Locale and Time Zone

For correct Collection Manager and Sybase operation, U.S. English locale (en_US) must be used.

7 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-24175-01