Managing the SCMP

Revised: December 23, 2013, OL-30623-01

Introduction

This chapter provides an overview of the Service Control Management Protocol (SCMP) capabilities. It also explains the various procedures for configuring and monitoring SCMP.

About SCMP

The Service Control Management Protocol (SCMP) is a protocol that integrates the SCE platform and the ISG (Intelligent Service Gateway) functionality of the Cisco routers, thereby providing a mechanism that allows the ISG and the SCE platform to manage subscriber sessions together without requiring coordination and orchestration by additional components.

The SCMP is a Cisco proprietary protocol that uses the RADIUS protocol with CoA (Change of Authorization) support as a transport layer. The SCMP provides connection management messages, subscriber management and subscriber accounting messages. Each subscriber in the SCE platform represents a session in the SCMP peer (as defined by the ISG terminology).

Connection management

The SCE platform initiates the connection to the peer device. On SCMP connection establishment, the SCE platform and ISG negotiate the following details:

- Introduction mode – whether the SCMP peer must send a session-provisioning message on session creation.
- Keep-alive message interval
- Protocol version

Subscriber Management

The SCMP peers can work in either of two introduction modes. These introduction modes affect only how and when a session is created on the SCE platform:

- The SCMP peer provisions the session to the SCE platform when it is created in the peer device (push)
- The SCE platform queries the SCMP peer regarding unmapped IP traffic (pull).

The SCMP uses queries as a backup to the push introduction mode, to be robust to issues such as networking problems and SCE platform reboot.

In addition to session creation, the SCMP supports the following operations:

- Change of session policy and network IDs using the update-session message
- Removal of the session when the user logs-out
- Activate-policy, which changes the session policy
- Deactivate-policy, which sets the policy value of the related anonymous-group template (based on the session manager)

Subscriber Accounting

On session creation, the SCE platform sends an accounting start message for the session and on logout, it sends an accounting stop message for the session. In addition, for each SCA BB service-counter an accounting-session is maintained (start, interim and stop messages), which provides information regarding the relevant volume, flow-count and duration.

The accounting messages are based on the new Subscriber-Accounting RDR and are sent according to the interval defined in the PQB configuration.

SCMP Terminology

SCMP terminology is similar to, but not identical to, existing SCE platform terminology. It is derived from the ISG terminology, since every SCE subscriber is actually an ISG session.

- subscriber – The client who is purchasing service from the Service Provider and is receiving the bill.
- User – A member, employee or guest at the subscriber household or business using the service.
- Session – A logically identifiable entity on the service gateway that represents communication with a peer. It is based on a unique combination of one or more Identity Keys such as an IP address, a subnet, a MAC address, a tunnel termination interface (PPP) or a port.

  Each session is assigned a unique identifier.
- Flow – Characterized by several parameters identifiable from the traffic such as source IP address, destination IP address, source port, destination port, protocol and in some cases direction.
- SCMP Peer – A Cisco device running IOS with the ISG module enabled.
- Identity Key – One of the keys that help identify a Session. The identity keys that are relevant to the SCE-ISG control-bus are:
  - IP Address/Subnet
  - IP Subnet
- Policy – Defines all aspects of subscriber session processing. A policy consists of conditions and actions. Traffic conditions will classify traffic and allow policing actions to be applied to the traffic. Policies may be provisioned, updated and removed. Policies may also be activated for a session or deactivated for a session. A policy may be referred to by name.

Deployment Scenarios

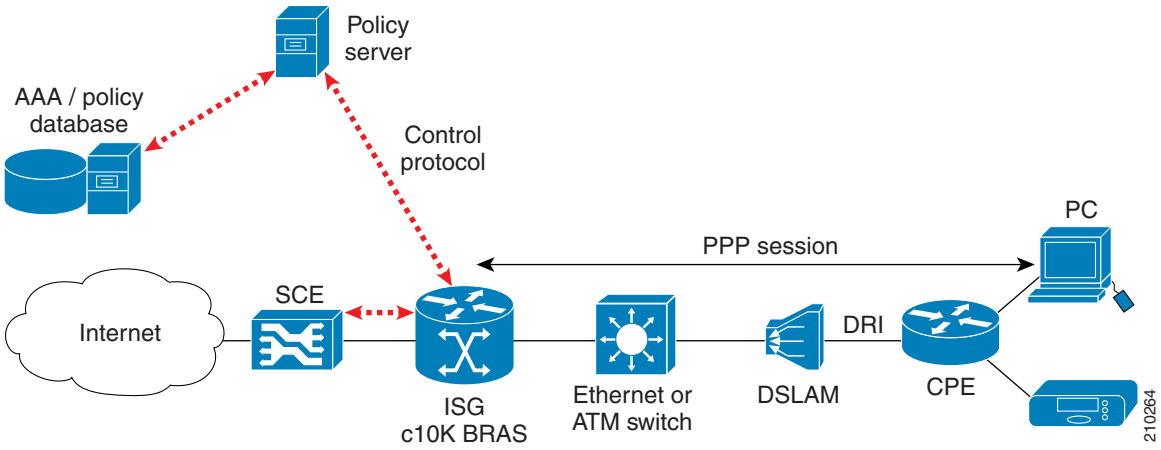
The following sections illustrate the basic types of SCMP deployment scenarios.

- 1xISG – 1xSCE
- 1xISG – 2xSCE (SCE cascade)
- NxISG – 2xSCE (SCE cascade)
- NxISG – MxSCE Via Load Balancing (MGSCP)

Single ISG Router with a Single SCE Platform (1xISG – 1xSCE)

Figure 14-1 illustrates a deployment using one ISG router with a single SCE platform.

Figure 14-1 Single ISG Router with a Single SCE Platform



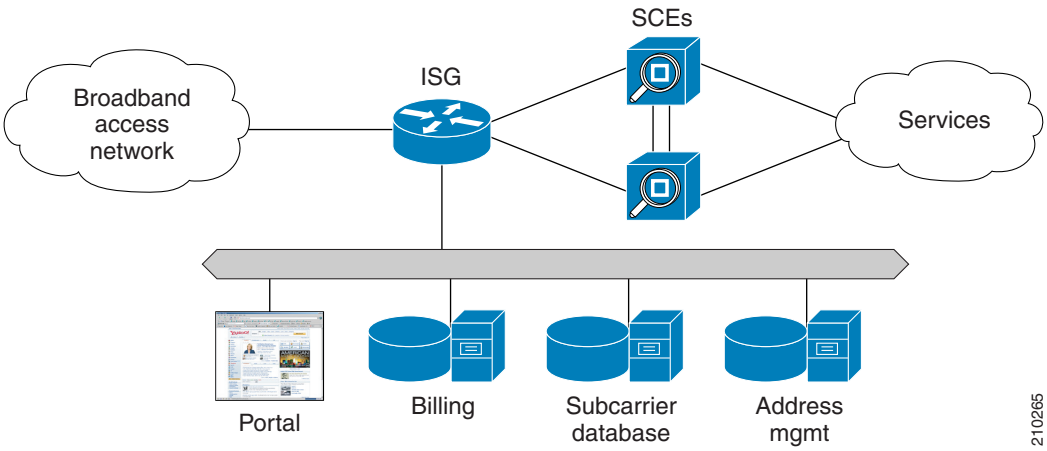
Note the following:

- The red dotted lines depict the control path communication.
- A deployment of this type might be used with ISG running on a service gateway or BRAS terminating a large number of subscribers. However, note that deploying only one SCE platform results in a single point of failure, which is not generally acceptable in an actual deployment.

Single ISG Router with Two Cascaded SCE Platforms (1xISG – 2xSCE)

Figure 14-2 illustrates a deployment using one ISG router with two cascaded SCE platforms.

Figure 14-2 Single ISG Router with Two Cascaded SCE Platforms



This scenario is similar to the previous one, with ISG running on a service gateway or BRAS terminating a large number of subscribers, however a second SCE platform has been added to provide redundancy. This redundancy scheme assumes that SCE platforms are connected in a cascade, with one active SCE platform and one backup.

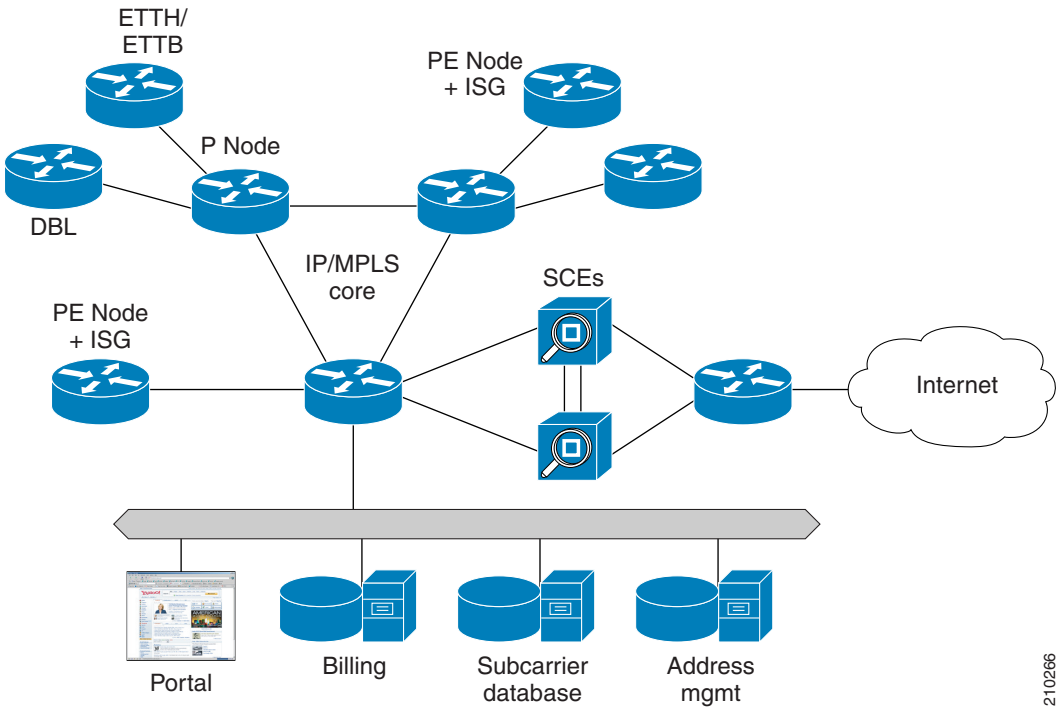
Please note the following:

- When cascaded SCE platforms are connected to one or more ISG devices, only the active SCE platform maintains a connection to the ISG devices.
- You can configure the cascaded SCE platforms to receive session info from the SCMP peer on session creation or pull the session info when the subscribers traffic traverses the SCE platform.
- An ISG device cannot push sessions to two SCE platforms at the same time

Multiple ISG Routers with Two Cascaded SCE Platforms (NxISG – 2xSCE)

Figure 14-3 illustrates a deployment using multiple ISG routers with two cascaded SCE platforms.

Figure 14-3 Multiple ISG Routers with Two Cascaded SCE Platforms



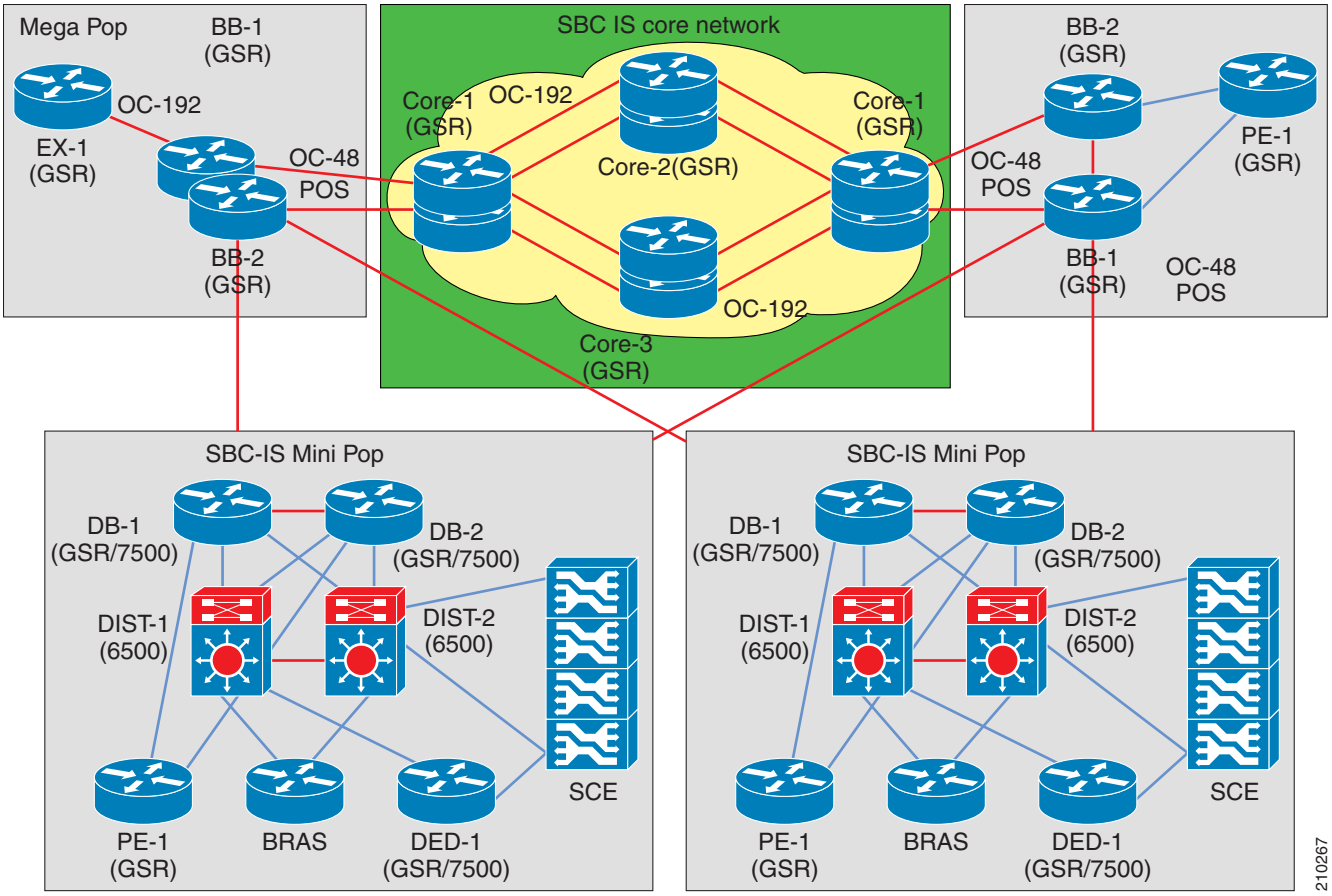
Many SPs require an edge platform with MPLS functionality to support L2 and L3 VPN services for business customers, with the possibility of running subscriber management functions for residential and business subscribers terminating on the same platform. If advanced services requiring deep packet inspection are offered, we recommend locating the SCE platforms centrally, just before traffic requiring such services exits the SP network, since not all traffic needs to be processed by SCE platforms. Please note the following:

- When cascaded SCE platforms are connected to one or more ISG devices, only the active SCE platform maintains a connection to the ISG devices.
- You can configure the cascaded SCE platforms to receive session info from the SCMP peer on session creation or pull the session info when the subscribers traffic traverses the SCE platform.
- An ISG device cannot push sessions to two SCE platforms at the same time.

Multiple ISG Routers with Multiple SCE Platforms via Load Balancing (NxISG – MxSCE)

Figure 14-4 illustrates a deployment using multiple ISG routers with multiple SCE platforms via load balancing. This is the scenario required for a MGSCP deployment.

Figure 14-4 Multiple ISG Routers with Multiple SCE Platforms via Load Balancing



This scenario includes several SCE platforms connected to the 7600/6500 switch. For efficient control of subscriber flows, the same SCE platform must process both directions of each subscriber flow, since the SCE platform keeps the subscriber context. The 7600/6500 switch to which the SCE platforms are connected acts as a dispatching element, distributing subscriber flows between SCE platforms and guaranteeing that all flows of a specific subscriber will pass through the same SCE platform.

This scenario assumes that one (or sometimes more) of the devices in the cluster is redundant.

Please note the following:

- An ISG device cannot push sessions to two SCE platforms at the same time.
- You must configure multiple SCE platforms with load-balancing (MGSCP) to work in pull integration mode.

SCMP Peer Devices

An SCMP peer device is a Cisco device running IOS with the ISG module enabled. The SCE platform supports the ability to communicate with several SCMP peer devices at the same time. However, each peer device manages its own subscribers and the corresponding subscriber network IDs. The SCE platform recognizes which subscribers belong to which peer device. There are two mechanisms that accomplish this:

- Login operation

  Each SCMP peer device is assigned a unique ID called the Manager-Id. This ID is attached to each subscriber from the moment it is created in the subscriber database, based on the SCMP peer that logged-in the subscriber.

- Anonymous groups

  An anonymous group is a specified IP range, possibly assigned a subscriber template (see Anonymous Groups and Subscriber Templates, page 9-7).

  SCMP associates each SCMP peer device with at least one anonymous group. SCMP generates subscribers for this anonymous group when it detects traffic from the SCMP peer device that is not mapped to any subscriber. SCMP assigns the SCMP peer manager-Id to this generated anonymous-subscriber. If you have assigned a subscriber template to the group, the anonymous subscribers generated have properties as defined by that template. If you have not assigned a subscriber template, the default template is used.

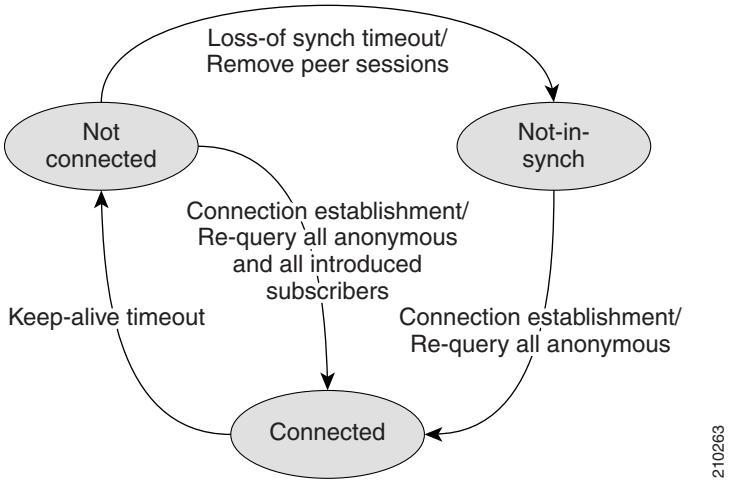
One SCE platform supports a maximum of 20 SCMP peer devices.

Connection Management

The SCMP attempts to maintain an open connection to each peer device.

Figure 14-5 illustrates the SCMP connection state functionality.

Figure 14-5 SCMP Connection State Functionality



The loss-of-sync timeout prevents the SCE platform from retaining sessions that are obsolete and whose identity-keys have been replaced or moved to other sessions thus miss-classification risk is limited.

SCMP Subscriber Management

Subscriber virtualization allows multiple SCMP peer devices to simultaneously manage subscribers in the SCE platform without interfering with each other. (Note that each device must handle a distinct set of subscribers and network IDs.)

The following mechanisms support subscriber virtualization:

- SCMP adds the Manager-Id field to each subscriber record in the database.
- All SCMP subscriber provisioning operations include the Manager-Id parameter for each subscriber.
- SCMP performs synchronizations in the context of the Manager-Id.
- SCMP dispatches queries according to the configuration of the anonymous subscriber groups.

GUID and Subscriber ID

The SCMP requires the use of a globally unique identifier (GUID) that is created by and identifies each SCMP peer device. The GUID is a 16-character-long ASCII string. The SCE platform uses the GUID for all communication with the SCMP peer.

SCMP creates the SCE subscriber ID from the concatenation of any or all the following user-related RADIUS attributes, with the GUID as the suffix.

- Calling-Station-Id
- NAS-port-Id
- User-Name

The user defines this subscriber ID structure via CLI.

Configuring SCMP

Configuring SCMP Parameters

You can configure the following options for the SCMP:

- Enable the SCMP
- Configure the SCMP peer device to push sessions to the SCE platform
- Allow the SCMP peer device to provision each subscriber to only one SCE platform.
- Define the SCMP keep-alive interval
- Define the SCMP reconnect interval
- Define the loss-of-sync timeout
- Define the subscriber ID structure

How to Enable the SCMP

By default, the SCMP is disabled.

Step 1 From the SCE(config)# prompt, type **scmp** and press **Enter**.

How to Disable the SCMP

Step 1 From the SCE(config)# prompt, type **no scmp** and press **Enter**.

Configuring the SCMP Peer Device to Push Sessions

When SCMP establishes a connection with an SCMP peer device, it informs the device whether the SCMP is configured to push sessions or to wait till the sessions are pulled by the SCE platform.

Use this command to specify push mode. Use the no form of the command to specify pull mode. This configuration takes effect only after the connection is re-established.

Default is disabled (pull mode).

Step 1 From the SCE(config)# prompt, type **scmp subscriber send-session-start** and press **Enter**.

How to Disable Pushing Sessions

Use this command to disable pushing sessions to the SCE platform. This means that the SCE platform will pull all sessions from the SCMP peer.

Step 1 From the SCE(config)# prompt, type **no scmp subscriber send-session-start** and press **Enter**.

Configuring the SCMP Peer Device to Force Each Subscriber to a Single SCE Platform

When SCMP establishes a connection with an SCMP peer device, it informs the device whether the SCMP is configured to allow each subscriber to be provisioned to only one SCE platform.

Use this command to configure the SCMP peer device to verify that each subscriber is provisioned to only one SCE platform. If a subscriber was provisioned to a different SCE platform, the SCMP removes it from the previous SCE platform and provisions it to the new SCE platform. This configuration is required in MGSCP topology where, if a fail-over between SCE platforms, subscribers might move from one SCE platform to another. If transferred subscribers are not cleared from the previous SCE platform, it can cause capacity issues.

Use the **no** form of the command to allow SCMP to provision subscribers to more than one SCE platform.

This configuration takes effect only after the connection is re-established.

Default is disabled (subscribers can be provisioned to more than one SCE platform).

Step 1 From the SCE(config)# prompt, type **scmp subscriber force-single-sce** and press **Enter**.

How to Disable Forcing Each Subscriber to a Single SCE Platform

Use this command to disable forcing each subscriber to only one SCE platform. This allow subscribers to be provisioned to more than one SCE platform.

Step 1 From the SCE(config)# prompt, type **no scmp subscriber force-single-sce** and press **Enter**.

How to Define the Keepalive Interval Parameter

The keepalive interval is the amount of time between keepalive messages to the SCMP peer device. If the SCMP does not receive a response from the SCMP peer device within the defined interval, the connection is assumed to be down; and the SCMP changes the connection state to false and begins attempts to reconnect.

Options

The following options are available:

- **interval** — Interval between keep-alive messages from the SCE platform to the SCMP peer device in seconds
  - Default = 5 seconds

Step 1 From the SCE(config)# prompt, type **scmp keepalive-interval** *interval* and press **Enter**.

How to Define the Reconnect Interval Parameter

The reconnect interval is the amount of time between attempts by the SCE platform to reconnect with an SCMP peer. The SCE platform attempts to reconnect to the SCMP peer device at the defined intervals by sending an establish-peering-request message.

Options

The following options are available:

- **interval** — Interval between attempts by the SCE platform to reconnect with an SCMP peer, in seconds
  - Default = 30 seconds

Step 1 From the SCE(config)# prompt, type **scmp reconnect-interval** *interval* and press **Enter**.

How to Define the Loss-of-Sync Timeout Parameter

The loss of sync timeout interval is the amount of time between loss of connection between the SCE platform and an SCMP peer device and the loss-of-sync event. (To prevent miss-classification, loss-of-sync event removes all subscribers that were provisioned by the relevant SCMP peer device.)

Options

The following options are available:

- **interval** — Loss of sync timeout interval in seconds
  - Default = 90 seconds

Step 1 From the SCE(config)# prompt, type **scmp loss-of-sync-timeout** *interval* and press **Enter**.

Adding an SCMP Peer Device

Adding an SCMP peer device is a two-step process:

1. Define the device, configuring the following parameters:
   - device name
   - RADIUS host
   - RADIUS shared secret authorization
   - port number (optional)
   - accounting port number (optional)
2. Associate the device with one or more unmapped anonymous groups.

How to Define an SCMP Peer Device

Options

The following options are available:

- **peer_device_name** — User-assigned name of the SCMP peer device
- **radius_hostname** — IP address or host-name of the RADIUS host (if a host-name is used, it must be valid at time of the configuration)
- **shared_secret** — RADIUS shared secret
- **auth-portnumber** (optional) — authorization port number
- **acct-portnumber** (optional) — accounting port number

Defaults:

- auth-port# — 1812
- acct-port# — 1813

Step 1 From the SCE(config)# prompt, type **scmp name** *peer_device_name* **radius** *radius_hostname* **secret** *shared_secret* **[auth-port** *auth-portnumber* **acct-port** *acct-portnumber***]** and press **Enter**.

Assigning the SCMP Peer Device to an Anonymous Group

This command defines the specified anonymous group to be the IP range of the SCMP peer device. You must define the specified SCMP peer device before assigning the anonymous group.

Options

The following options are available:

- **group-name** — Name of the anonymous subscriber group to be associated with the specified SCMP peer device.
- **range** (optional) — IP range defined for the anonymous group
- **template** (optional) — group template assigned to the anonymous group
- **peer-device-name** — User-assigned name of the SCMP peer device

Step 1 From the SCE(config if)# prompt, type **subscriber anonymous-group name** *group-name* **IP-range** *range* **[template** *template***] scmp name** *peer-device-name* and press **Enter**.

How to Remove an Anonymous Group from the SCMP Peer Device

This command defines the specified anonymous group to be the IP range of the SCMP peer device. You must define the specified SCMP peer device before assigning the anonymous group.

Step 1 From the SCE(config if)# prompt, type **no subscriber anonymous-group name** *group-name* and press **Enter**.

Deleting Subscribers Managed by an SCMP Peer Device

Use this command to clear all the subscribers that are managed by a specified SCMP peer device.

Options

The following options are available:

- **peer_device_name** — User-assigned name of the SCMP peer device

Step 1 From the SCE(config if)# prompt, type **no subscriber scmp name** *peer-device-name* **all** and press **Enter**.

Deleting an SCMP Peer Device

You cannot delete an SCMP peer device that has anonymous groups assigned to it. You must remove all associated anonymous groups before deleting the device.

Step 1 First remove all anonymous groups assigned to the device:

```
SCE(config if)# no subscriber anonymous-group name group-name [IP-range range][template
template] scmp name peer-device-name
```

Step 2 Repeat this step for all anonymous groups assigned to the SCMP peer device.

Step 3 When all anonymous groups have been removed from the device, exit LineCard Interface Configuration mode

```
SCE(config if)# exit
```

Step 4 Delete the device

```
SCE(config)#no scmp name peer_device_name
```

Defining a Subscriber ID

You can define the structure of the subscriber ID via this command by specifying which of the following elements to include and in which order:

- Calling-Station-Id
- NAS-port-Id
- User-Name

The GUID is always appended at the end of the subscriber ID as defined by this command.

Note You must disable the SCMP interface before executing this command.

Options

The following options are available:

- 1st element — any one of the following:
  - Calling-Station-Id
  - NAS-Port-Id
  - User-Name
- 2nd element (optional) — any one of the following (if specified, usually not the option specified as the first element):
  - Calling-Station-Id
  - NAS-Port-Id
  - User-Name
- 3rd element (optional) — any one of the following (if specified, usually the remaining option not specified as either of the first two elements):
  - Calling-Station-Id
  - NAS-Port-Id
  - User-Name

Default = no elements concatenated with the GUID

Step 1 Disable the SCMP.

```
SCE(config)#no scmp
```

Step 2 Define the subscriber ID:

```
SCE(config)#scmp subscriber id append-to-guid radius-attributes Calling-Station-Id |
NAS-Port-Id | User-Name [Calling-Station-Id | NAS-Port-Id | User-Name] [Calling-Station-Id
| NAS-Port-Id | User-Name]
```

Step 3 Enable the SCMP.

```
SCE(config)#scmp
```

Configuring the RADIUS Client

You can configure the following options for the RADIUS client

- Define the parameters for retransmitting unacknowledged messages.

The RADIUS client polls the sockets to receive the next message and calls the SCMP engine to handle it, based on the type of the received message. Messages that were not acknowledged can be retransmitted up to the configured maximum number of retries.

Options

The following options are available:

- **times** — The maximum number of times the RADIUS client can try unsuccessfully to send a message.
  - Default = 3
- **timeout** (optional) — Timeout interval for retransmitting a message, in seconds
  - Default = 1 second

Step 1 From the SCE(config)# prompt, type **ip radius-client retry limit times [timeout** *timeout*] and press **Enter**.

Monitoring the SCMP Environment

You can monitor the following components of the SCMP environment:

- SCMP
- RADIUS client

Monitoring the SCMP

Use the following commands to monitor the SCMP. These commands provide the following information:

- General SCMP configuration
- Configuration of all currently defined SCMP peer devices.
- Configuration of a specified SCMP peer device.
- Statistics for either all SCMP peer devices or a specified SCMP peer device.

Options

The following options are available:

- **device-name** — The name of the specific SCMP peer device for which to display the configuration or statistics.

How to Display the General SCMP Configuration

Step 1 From the SCE> prompt, type **show scmp** and press **Enter**.

Example

```
SCE> show scmp

SCMP enabled:                    yes
Keep-alive interval:             5 seconds
Loss of synchronization timeout: 90 seconds from disconnection
Reconnection interval:           30 seconds
Force subscriber on a single SCE: no
Peer sends subscriber data on session start
Subscriber Id structure: GUID
```

How to Display the Configuration All the Currently Defined SCMP Peer Devices

Step 1 From the SCE> prompt, type **show scmp all** and press **Enter**.

How to Display the Configuration for a Specified SCMP Peer Device

Step 1 From the SCE> prompt, type **show scmp name** *device-name* and press **Enter**.

Example

```
SCE>show scmp name isg
SCMP Connection 'isg' status:
10.56.208.91 auth-port 1812 acct-port 1813
Connection state:      Connected
Peer protocol-version: 1.0
Keep-alive interval:   5 seconds
Force single SCE:      No
Send session start:    Yes
Time connected:        9 seconds
```

How to Display The Statistics For All SCMP Peer Devices

Step 1 From the SCE> prompt, enter **show scmp all counters** and press **Enter**.

How to Display The Statistics For A Specified SCMP Peer Device

Step 1 From the SCE> prompt, enter **show scmp name** *peer_device_name* **counters** and press **Enter**.

Example

```
SCE> show scmp name isg counters

SCMP Connection 'isg' counters:
Total messages sent:            72
Total messages received:        72
Establish requests sent:        1
Establish replies received:     1
Accounting requests sent:       20
Accounting replies received:    20
Subscriber queries sent:        0
Subscriber query response recv: 0
Request retry exceeded:         0
Requests replied with errors:   0
Subscriber requests received:   50
Subscriber responses sent:      50
Failed Requests:                0
Keep-alive sent:                1
Keep-alive received:            1
```

Monitoring the RADIUS Client

Use the following command to monitor the SCMP RADIUS client. This command displays the general configuration of the RADIUS client.

Step 1 From the SCE> prompt, type **show ip radius-client** and press **Enter**.