



## **Cisco SCMS SM SCE-Sniffer DHCP LEG**

### **Reference Guide**

Version 3.0  
OL-8235-01

**Corporate Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Customer Order Number: DOC-823501=  
Text Part Number: OL-8235-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCI, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Printed in the USA on recycled paper containing 10% postconsumer waste.

*Cisco SCMSSM SCE-Sniffer DHCP LEG Reference Guide*

Copyright © 2005 Cisco Systems, Inc.  
All rights reserved.



## **Preface iii**

- Document Revision History iii
- Audience iii
- Organization iv
- Related Documentation iv
- Conventions iv
- Obtaining Documentation v
  - World Wide Web v
  - Documentation CD-ROM vi
  - Ordering Documentation vi
  - Documentation Feedback vi
- Obtaining Technical Assistance vii
  - Cisco.com vii
  - Technical Assistance Center vii

## **About the SCMS SM SCE-Sniffer DHCP LEG 1-1**

- The SCE-Sniffer DHCP LEG Module 1-2
- Terms and Concepts 1-2
  - LEG (Login Event Generator) 1-2
  - RDR (Raw Data Record) 1-3
  - Cable/Satellite Modem 1-3
  - CPE (Customer Premise Equipment) 1-3
  - DHCP ACK packet 1-3
  - DHCP initial logon transaction 1-3
  - DHCP lease extension transaction (renewal) 1-3
  - DHCP release transaction 1-3
  - DHCP Sniffer 1-3
  - Subscriber Mappings 1-4
  - Subscriber Domain 1-4

Subscriber Package 1-4

**SCE-Sniffer DHCP LEG Functionality 2-1**

DHCP initial login transaction 2-1

DHCP lease extension transaction 2-2

DHCP release transaction 2-2

**Installing the SCE-Sniffer DHCP LEG 3-1**

Installing the SCE-Sniffer DHCP LEG Module 3-1

Uninstalling the SCE-Sniffer DHCP LEG 3-3

Upgrading the SCE-Sniffer DHCP LEG 3-4

**Configuring the SCE-Sniffer DHCP LEG 4-1**

Configuring the General Settings 4-1

Example 4-2

Configuring the Package Association 4-2

Dynamic Assignment of Package Information 4-3

Static Assignment of Package Information 4-4

**Using the SCE-Sniffer DHCP LEG CLU 5-1**

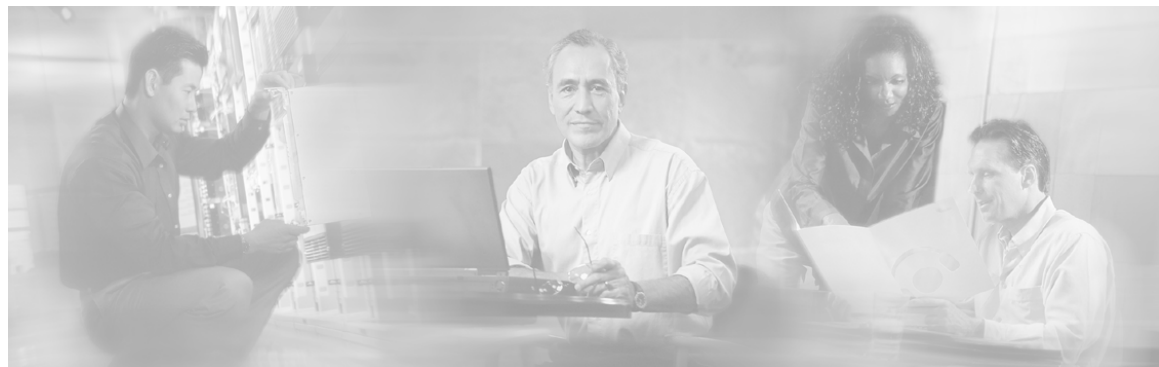
p3dhcpsniff Utility 5-1

Viewing the SCE-Sniffer DHCP LEG Status 5-2

Viewing the SCE-Sniffer DHCP LEG Statistics 5-2

Viewing the SCE-Sniffer DHCP LEG Version 5-2

**Index I-1**



## Preface

---

This document describes the concept of a DHCP Login Event Generator (LEG) based on an RDR server, and explains how to install and configure it on the SCMS Subscriber Manager (SM) platform.



---

**Note** This document assumes a basic familiarity with the Cisco SCMS subscriber management, subscriber integration concepts, and the DHCP protocol.

---

For complete information regarding Cisco's subscriber integration concept, see the *SCMS Subscriber Manager User Guide*.

## Document Revision History

Cisco Service Center Release	Part Number	Publication Date
Release 3.0	OL-8235-01	December, 2005

### Description of Changes

New Subscriber Manager component release.

## Audience

This document is intended for system administrators and system integrators who are familiar with the SCE-Sniffer DHCP LEG concepts and with Cisco Service Control Subscriber Management and Subscriber Integration concepts.

## Organization

This guide contains the following topics:

Chapter	Title	Description
Chapter 1	<i>About the SCMS SM SCE-Sniffer DHCP LEG</i> (on page 1-1)	Describes the Subscriber Manager SCE-Sniffer DHCP LEG software module and the terms and concepts used in this guide.
Chapter 2	<i>SCE-Sniffer DHCP LEG Functionality</i> (on page 2-1)	Provides a description of the SCE-Sniffer DHCP LEG operation and transactions.
Chapter 3	<i>Installing the SCE-Sniffer DHCP LEG</i> (on page 3-1)	Details the procedures for installing the software on the Subscriber Manager. It also describes uninstalling the software and upgrading procedures.
Chapter 4	<i>Configuring the SCE-Sniffer DHCP LEG</i> (on page 4-1)	Describes the configuration procedure for the SCE-Sniffer DHCP LEG on the SM and configuring the Package Association.
Chapter 5	<i>Using the SCE-Sniffer DHCP LEG CLU</i> (on page 5-1)	Provides a description of the command-line utility commands when the software is installed on the Subscriber Manager.

## Related Documentation

This *SM SCE-Sniffer DHCP LEG* Reference Guide should be used in conjunction with the following Cisco documentation:

- *SCMS Subscriber Manager User Guide*
- *Service Control Application for Broadband (SCA BB) User Guide*

## Conventions

This document uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands and keywords are in <b>boldface</b> .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{x   y   z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x   y   z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.

screen font	Terminal sessions and information the system displays are in screen font.
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled <b>Control</b> —for example, the key combination <b>^D</b> in a screen display means hold down the <b>Control</b> key while you press the <b>D</b> key.
< >	Non printing characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:




---

#### Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

---

Cautions use the following conventions:




---

#### Caution

Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

---

Warnings use the following conventions:




---

#### Warning

Means *reader be warned*. You are capable of doing something that might result in bodily injury.

---

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>

- <http://www-europe.cisco.com>

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the networking Products MarketPlace:

[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

<http://www.cisco.com/pcgi-bin/marketplace/welcome.pl>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can email your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.



# Obtaining Technical Assistance

Cisco provides *Cisco.com* (on page [vii](#)) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for *Cisco.com* (on page [viii](#)), go to the following website:

*<http://tools.cisco.com/RPF/register/register.do>*

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

*<http://www.cisco.com/tac/caseopen>*

## Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

*<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>*

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



## About the SCMS SM SCE-Sniffer DHCP LEG

---

The SCMS SM SCE-Sniffer DHCP LEG is a software module that receives RDR (Raw Data Record) messages containing DHCP information from SCE devices configured with a DHCP sniffer service. The SCE-Sniffer DHCP LEG is an extension of the Subscriber Manager (SM) software and runs as part of the SM.

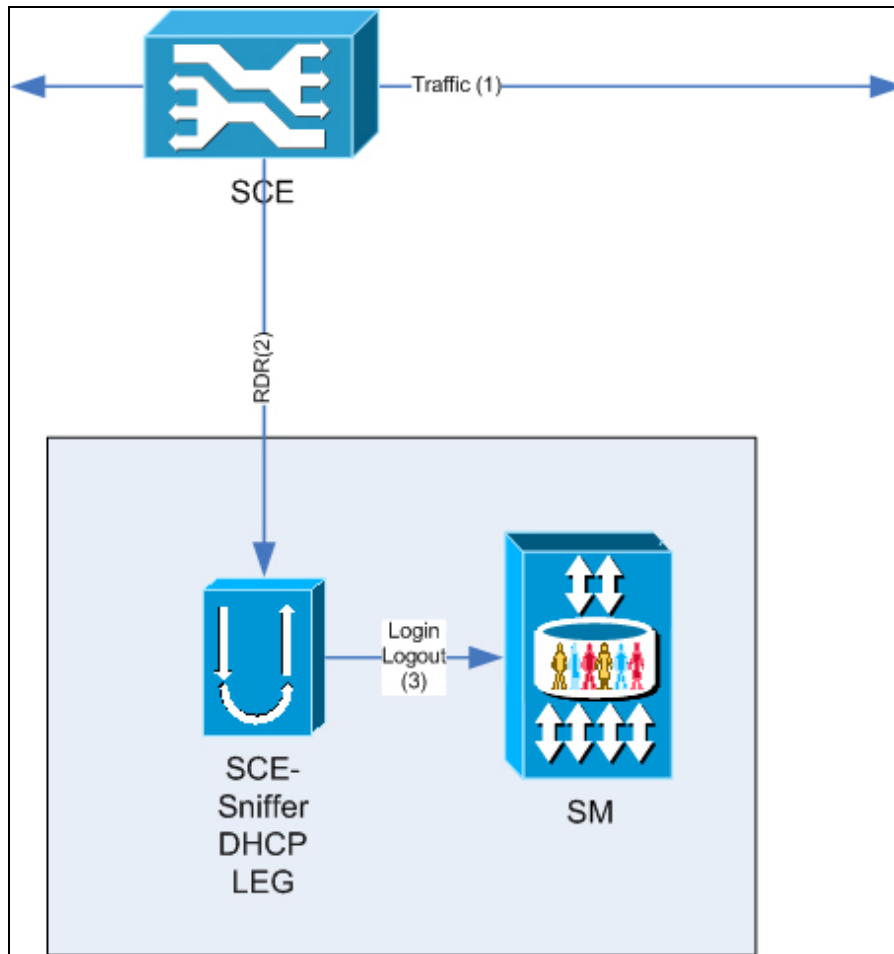
This chapter contains the following sections:

- [The SCE-Sniffer DHCP LEG Module](#) 1-2
- [Terms and Concepts](#) 1-2

## The SCE-Sniffer DHCP LEG Module

The SCE device analyzes DHCP traffic, and reports the DHCP transactions to the SM device using the RDR protocol. The SM extracts the modem MAC address, the CPE IP address, and optionally, the subscriber package information from the RDR, and triggers a login or logout operation to the SM.

The following diagram represents the operation of the SCE-Sniffer DHCP LEG:



## Terms and Concepts

The following is a list of terms and concepts that are necessary to understand the SCE-Sniffer DHCP LEG and SM configuration and operation. Additional information regarding the various issues can be found in the *SCMS Subscriber Manager User Guide*.

### LEG (Login Event Generator)

A software component that performs subscriber login and logout operations on the SM and is used to handle dynamic subscriber integration.

## RDR (Raw Data Record)

A client/server data protocol that enables the SCE devices to export reports about network transactions to external collectors. This is a Cisco proprietary protocol.

## Cable/Satellite Modem

A data modem that provides Internet access over Cable and Satellite networks. The modem usually corresponds to a single subscriber of the Internet Service Provider (ISP).

## CPE (Customer Premise Equipment)

Any equipment that an end-user can connect to the network through a modem. The end-user usually owns multiple CPE devices that are used to connect to the Internet through a single modem.

## DHCP ACK packet

The final packet that is transmitted from the DHCP server in each DHCP transaction (except the release transaction). After the transmission of the DHCP ACK packet, the results of the transaction are final.

## DHCP initial logon transaction

A DHCP transaction for an initial logon of a network entity to the network. The purpose of the transaction is to assign an IP address to the newly connected entity. Because the modem MAC address is used as the subscriber name, the modem MAC address will be added by the DHCP relay agent during the initial logon query using option 82 (Remote-ID sub-option of the DHCP Relay Agent Information Option).

## DHCP lease extension transaction (renewal)

A DHCP transaction for renewal of the entity lease time. When the lease time has been reached, the network entity is removed from the network. The LEG uses this query to logon the subscriber using the new lease time.

## DHCP release transaction

A DHCP transaction for releasing IP addresses. This transaction is used to logout network entities from the network. The DHCP release transaction is rarely used. Logout is usually performed when the lease time expires, and not directly with a release transaction. The LEG uses the release query to logout a subscriber from the SM.

## DHCP Sniffer

The software logic inside the SCE device that analyzes DHCP traffic and sends the information to the SCE-Sniffer DHCP LEG using the RDR protocol.

## Subscriber Mappings

The SCE platform requires mappings between the network IDs (IP addresses) of the flows it encounters and the subscriber IDs. The SM database contains the network IDs that map to the subscriber IDs. The SCE network-ID-to-subscriber mappings are constantly updated from the SM database.

The main function of the SCE-Sniffer DHCP LEG is to provide the SM with network-ID-to-subscriber mappings in real time.

## Subscriber Domain

The SM provides the option of partitioning SCE platforms and subscribers into subscriber domains. A subscriber domain is a group of SCE platforms that share a group of subscribers. Subscriber domains can be configured using the SM configuration file and can be viewed using the SM Command-Line Utility (CLU).

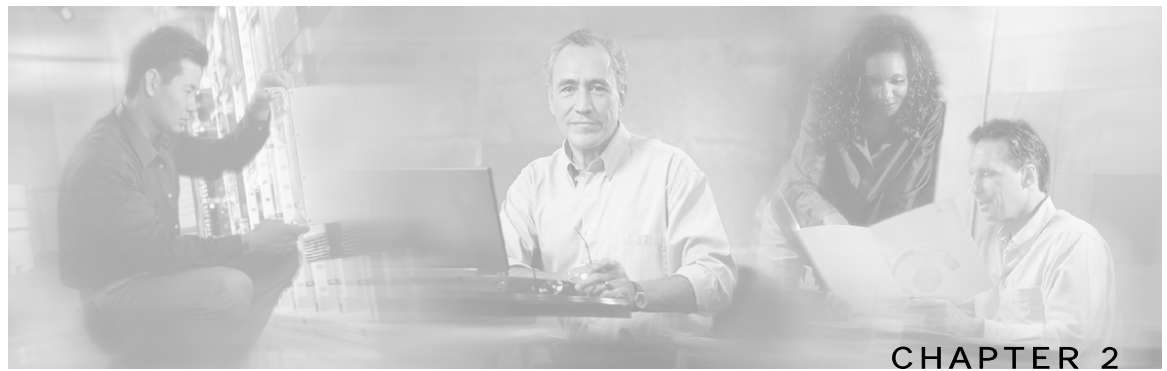
For additional information about domains and domain aliases, see *Appendix A* of the *SCMS Subscriber Manager User Guide*.

## Subscriber Package

The policy enforced by Cisco solutions on a certain subscriber is usually defined by a policy subscriber package. The SCE-Sniffer DHCP LEG can handle the package ID in any of the following ways:

- Set according to configurable options of the DHCP initial logon or lease extension transactions
- Set using a constant default value
- Do not set the package ID.

For additional information, see *Configuring the Package Association* (on page 4-2) and the *Service Control Application for Broadband User Guide*.



## SCE-Sniffer DHCP LEG Functionality

The SCE devices analyze the DHCP ACK packets of DHCP transactions and sends the information to the SCE-Sniffer DHCP LEG that resides on the Subscriber Manager. The LEG performs login or logout operations to the SM using the information sent from the SCE devices. The DHCP transactions that are relevant for the operation of the LEG are *initial login*, *lease extension*, and *release*.

This chapter contains the following sections:

- [DHCP initial login transaction 2-1](#)
- [DHCP lease extension transaction 2-2](#)
- [DHCP release transaction 2-2](#)

### DHCP initial login transaction

The following is a detailed description of the attributes extracted from the *DHCP initial login transaction*:

- **Subscriber ID**—The modem MAC address is used as the subscriber ID. The information of the modem MAC address is extracted from option 82 (Remote-ID sub-option of the DHCP Relay Agent Information Option). Therefore, for a successful logon operation, it is required that option 82 will contain the modem MAC address in the DHCP initial logon transaction. If option 82 is missing, no login operation is performed.
- **IP address**—Each subscriber might have multiple IP addresses, depending on the number of CPE devices connected to the modem. A logon operation is triggered for each *assigned IP* in the DHCP message.

If the transaction correlates to a CPE device, the assigned IP for that CPE is added to the SM database. The IP address of the modem is not added to the SM database. If the transaction correlates to a modem device, no IP mappings are added to the SM database, but a login operation is performed anyway to update package information.

- **Lease time**—If the transaction correlates to a CPE device, the assigned IP is added to the SM database with a lease time taken from option 51 (lease time option). Note that option 51 must contain the lease time, otherwise no login is performed.

## DHCP lease extension transaction

- **Package**—The package information is assigned according to configurable options in the DHCP message. The LEG includes a component that converts the package information data from the DHCP packet to a subscriber package ID. If the package information is not found in the packet, it is possible to log in the subscriber with a default package, or log in the subscriber with no package information at all.

After extracting the above information, the LEG performs a login operation to the SM.

## DHCP lease extension transaction

The same attributes are extracted from the *DHCP lease extension transaction*, but the existence of option 82 is not required. If the modem MAC address cannot be retrieved from option 82, the SM database is queried for this information.

## DHCP release transaction

The *DHCP release transaction* is handled differently. If the transaction correlates to a CPE device, the LEG performs an SM logout operation with the IP address of the CPE, which appear as a released IP in the packet itself.



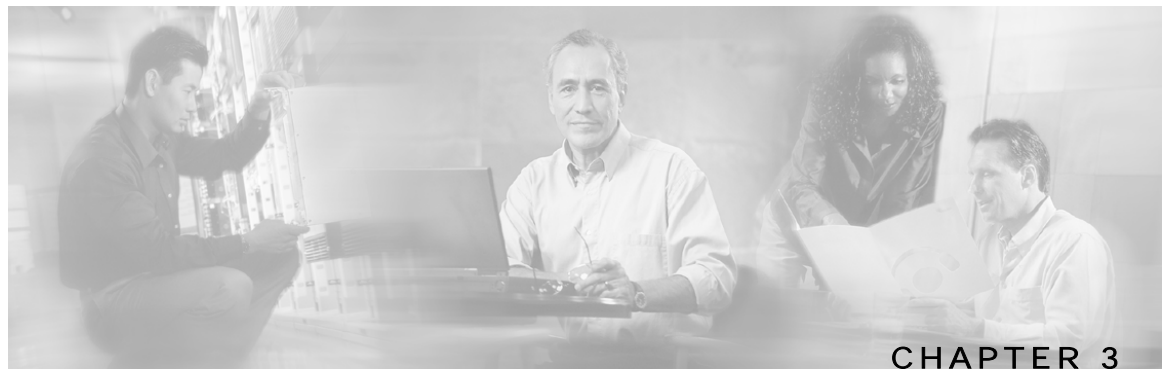
---

**Note**

To handle release transactions, it is required to configure the LEG to also handle DHCP Release packets. By default, the LEG only handles DHCP ACK packets.

---





## Installing the SCE-Sniffer DHCP LEG

This section describes the procedures for installing the SCE-Sniffer DHCP LEG. It also describes the uninstall procedure.

The SCE-Sniffer DHCP LEG is provided as an external component (PQI file) of the SM software and should be installed separately using the SM Command-Line Utility (CLU). The SCE-Sniffer DHCP LEG distribution is part of the SM LEG distribution.

The installation package of the LEG includes a set of configuration files and CLU commands for the SCE-Sniffer DHCP LEG.

This chapter contains the following sections:

- [Installing the SCE-Sniffer DHCP LEG Module](#) 3-1
- [Uninstalling the SCE-Sniffer DHCP LEG](#) 3-3
- [Upgrading the SCE-Sniffer DHCP LEG](#) 3-4

## Installing the SCE-Sniffer DHCP LEG Module



**Note** Verify that the Service Control Application for Broadband (SCA BB) is installed on all SM and SCE devices. If not, install the application as described in the *Service Control Application for Broadband User Guide*.



**Note** After the installation of the PQI file, the Subscriber Manager restarts automatically.

To Install the SCE-Sniffer DHCP LEG:

**Step 1** Install the PQI file of the SCE-Sniffer DHCP LEG

Run the **p3inst** command-line utility from the SM CLU `<sm-inst-dir>/sm/server/bin` (*sm-inst-dir* refers to the SM installation directory):

```
> p3inst --install -f dhcpsnif.pqi
```

**Step 2** Edit the configuration files of the SCE-Sniffer DHCP LEG. The SCE-Sniffer DHCP LEG includes 2 configuration files under `<sm-inst-dir>/sm/server/root/config`:

- a) `dhcpsnif.cfg` - configures general attributes of the LEG
- b) `dhcp_pkg.cfg` - configures rules for package assignment

---

**Note:** It is recommended to familiarize yourself with these files immediately after the first installation and edit them according to your specific needs. See *Configuring the SCE-Sniffer DHCP LEG* (on page 4-1) for more information.

---

**Step 3** Load the configuration files to the SM:

Run the **p3sm** command line utility from the SM CLU:

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

This command-line utility loads the new configuration to the SM and activates it.

**Step 4** Configure the SCE to send RDRs to the LEG:

Run the RDR-formatter CLI on the SCE platform to add the LEG as a category 3 RDR destination:

```
SCE2000> configure
SCE2000(config)> RDR-formatter destination <SM-IP> port <port> category
number 3 priority 100
SCE2000(config)> exit
```

Use the same port number as defined by the RDR server in the SM. The default port number is 33001.

---




---

**Note** To support SM cluster topology, set the cluster VIP as the SM-IP in the CLI above.

---

## Uninstalling the SCE-Sniffer DHCP LEG

To uninstall the SCE-Sniffer DHCP LEG:

---

**Step 1** Remove the configuration of the RDR formatter.

Run the RDR-formatter CLI on the SCE platform to remove the LEG as a category 3 RDR destination:

```
SCE2000> configure
SCE2000(config)> no RDR-formatter destination <SM-IP> port <port>
SCE2000(config)> exit
```

**Step 2** Uninstall the SCE-Sniffer DHCP LEG module.

Run the **p3inst** command-line utility from the SM CLU:

```
> p3inst --uninstall -f dhcpsnif.pqi
```

---



---

**Note** After the uninstall process, the Subscriber Manager restarts automatically.

---

## Upgrading the SCE-Sniffer DHCP LEG

The SCE-Sniffer DHCP LEG must be upgraded as part of the SM upgrade process, because previous versions of the SCE-Sniffer DHCP LEG are incompatible with the SM 3.0 version. The upgrade for the SCE-Sniffer DHCP LEG should be performed together with the upgrade process of the SM.

To upgrade the SCE-Sniffer DHCP LEG:

---

**Step 1** Backup the configuration files of the SCE-Sniffer DHCP LEG. The original configuration files are deleted by the uninstall process in the next step.

**Step 2** Uninstall the SCE-Sniffer DHCP LEG by running the following CLU:

```
> p3inst --uninstall -f <sce-sniffer-dhcp-leg-pqi>
```

---

**Note:** After the uninstall process has successfully completed, the SM automatically restarts.

---

**Step 3** Perform an upgrade of the SM as described in the *SCMS Subscriber Manager User Guide*.

**Step 4** Install the new version of the SCE-Sniffer DHCP LEG by running the following CLU:

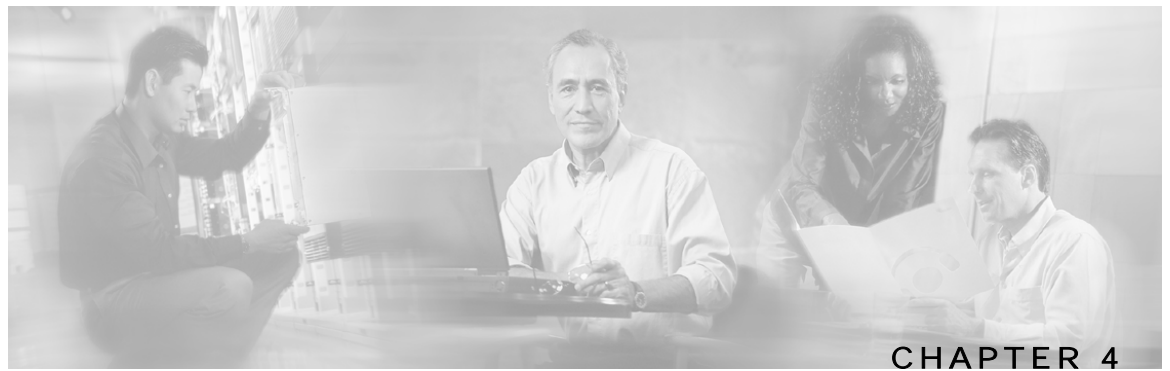
```
> p3inst --install -f <sce-sniffer-dhcp-leg-pqi>
```

**Step 5** Restore the configuration files of the SCE-Sniffer DHCP LEG.

**Step 6** Load the new configuration of the SM by running the following CLU:

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

---



## Configuring the SCE-Sniffer DHCP LEG

The SCE-Sniffer DHCP LEG is configured using two configuration files, *dhcpsnif.cfg* and *dhcp\_pkg.cfg*, which resides in the *sm-inst-dir/sm/server/root/config* directory (*sm-inst-dir* refers to the SM installation directory).

The configuration files consist of sections headed by a bracketed section title, for example `[RDR Server]`. Each section consists of several parameters having the format `parameter=value`. The number sign (“#”) at the beginning of a line signifies that it is a remark line.

The general configuration of the SCE-Sniffer DHCP LEG and the RDR server resides in *dhcpsnif.cfg*. The dynamic package association configuration resides in *dhcp\_pkg.cfg*.

This chapter contains the following sections:

- [Configuring the General Settings](#) 4-1
- [Configuring the Package Association](#) 4-2

### Configuring the General Settings

The following is a description of the configuration variables of *dhcpsnif.cfg*.

The `[SCE-Sniffer DHCP LEG]` section contains the following parameters:

- *start*  
Defines whether the SM should run the SCE-Sniffer DHCP LEG at startup. Possible values for this parameter are **yes** and **no**. The default value is **no**. To extract and handle the DHCP messages received by the RDR server, this parameter must be set to **yes**.
- *log\_failures*  
Defines whether the SM should add messages about failures to the user log. Possible values for this parameter are **true** and **false**. The default value is **true**.
- *log\_all*  
Defines whether the SM should add all messages, including successful logins and logouts, to the user log. Possible values for this parameter are **true** and **false**. The default value is **false**.

- *use\_default\_domain*

Defines whether the default domain “subscribers” should be used for all login operations.

Possible values for this parameter are **true** and **false**. The default value is **true**.

If the value is set to **false**, the SM will log in the subscribers using the domain name identical to the IP address of the SCE that received the DHCP traffic for that subscriber. In this case, you will have to configure domain aliases as described in *SCMS Subscriber Manager User Guide*.

The [Sniffer] section contains the following parameters:

- *packet\_types*

contains the DHCP packet types that should be sent to the LEG.

Possible values for this parameter are any combination of the following types: **DHCPACK**, **DHCPRELEASE**.

The default value is set to **DHCPACK** and **DHCPRELEASE**.



#### Note

For this LEG to work correctly, the RDR server must be enabled in the SM by using the configuration file.

## Example

The following is an example of a configuration file:

```
[SCE-Sniffer DHCP LEG]
start=yes
log_failures=true
log_all=false
use_default_domain=true

[Sniffer]
packet_types=DHCPACK
```

## Configuring the Package Association



#### Note

The configuration described in this section is optional.

Subscriber package configuration in the SCE-Sniffer DHCP LEG can be handled in any of the following ways:

- Dynamic assignment of package information using information extracted from the DHCP packet, See *Dynamic Assignment of Package Information* (on page 4-3).
- Static assignment of a constant package Id for all subscribers that log on via the SCE-Sniffer DHCP LEG, See *Static Assignment of Package Information* (on page 4-4).

## Dynamic Assignment of Package Information

Dynamic assignment of package information is supported if the package information is submitted in the DHCP packets. The LEG concatenates the desired options and creates a *package-name*. It is possible to map using the configuration between *package-names* and the application package-IDs.

To extract the package information data from the DHCP package, the configuration file *dhcp\_pkg.cfg* should define the option types that contain the package information and the conversion map of *package-names* to the package IDs of the Service Control Application for Broadband.

The [Package Association] section contains the following parameters:

- *options\_order\_for\_package\_name*  
Defines the DHCP options that contain the package association information and defines the order of concatenation of these option data. The option format must be defined as data type *string*.  
The format is `option[:subtype],option[:subtype]`
- *name\_separator\_value*  
Defines the separator character to use between each two options when concatenating them to each other to create the package name. Any character is accepted. The default value is the underscore character ("\_").
- *use\_default*  
Determines whether a default package should be used when no package information can be extracted from the DHCP data such as the configurable options are missing or no options were configured.  
Possible values are **true** or **false**. The default value is **true**.
- *default\_package*  
Defines the default package ID to use if no package information is extracted from the DHCP data. This parameter is relevant only if *use\_default* parameter is set to **true**.  
Possible value for this parameter is any integer number. This parameter has no default value.
- *allow\_login\_with\_no\_package*  
Defines whether a login without package information should be performed when no package information can be extracted from the DHCP data and the *use\_default* parameter is set to **false**.  
This parameter is relevant only if the *use\_default* parameter is set to **false**.  
Possible values are **true** or **false**. The default value is **false**.
- *package\_property\_name*  
Defines the name of the application property that contains the package information. The default value is the *packageID* as used by the SCA BB application.

The [Package Names] section contains the conversion information of the package information as it appears in the DHCP packet to the package ID number to be used by the SCA BB application.

## Example

Suppose that the package information appears inside option 43 (Vendor Specific Option) of the DHCP packet and both subtypes 102 and 101 are in use. The options order for package name should be configured as follows:

```
options_order_for_package_name=43:102,43:101
```

Suppose that option 43 with subtype 102 contains the type of package (gold, silver, or bronze) and option 43 with subtype 101 contains domain information (the package type has a different meaning in different domains). If the separator value is configured to the default value, the package names should be configured as follows:

```
[Package Names]
gold_domain1=11
gold_domain2=12
silver_domain1=13
silver_domain2=14
```

This configuration denotes that if the DHCP packet contains the value 'gold' inside option 43 with subtype 102, and the value 'domain1' inside option 43 with subtype 101, then the package ID that will be associated to the subscriber in the SM will have the value 11.

The following is an example of the entire configuration file:

```
[Package Association]
options_order_for_package_name=43:102,43:101
name_seperator_value=_
use_default=true
default_package=1
package_property_name=packageId

[Package Names]
gold_domain1=11
gold_domain2=12
silver_domain1=13
silver_domain2=14
```

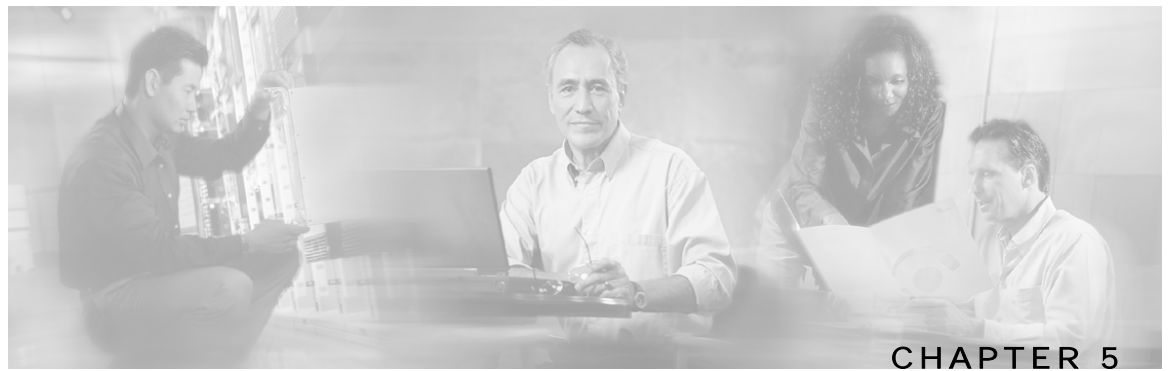
## Static Assignment of Package Information

If dynamic assignment of package information is not required by the installation, the configuration file *dhcp\_pkg.cfg* should define the default package ID to be assigned to all subscribers, as in the following example:

```
[Package Association]
use_default=true
default_package=1
```

All other configuration parameters should not be set.





## Using the SCE-Sniffer DHCP LEG CLU

---

This chapter contains the following sections:

- [p3dhcpsniff Utility 5-1](#)

### p3dhcpsniff Utility

The **p3dhcpsniff** utility is used to view the SCE-Sniffer DHCP LEG configuration, status, and statistics. The command format is **p3dhcpsniff <operation>**.

The following table lists the **p3dhcpsniff** operations.

Table 5-1 p3dhcpsniff Operations

Operation	Description
--show	Displays all of SCE-Sniffer DHCP LEG configurations and status
--show-statistics	Displays counters of DHCP messages handled and number of logon operations performed
--show-version	Displays the version information of the SCE-Sniffer DHCP LEG
--help	Displays a list of available operations and arguments, with a short explanation of their meanings.

## Viewing the SCE-Sniffer DHCP LEG Status

The following is an example using the `p3dhcpsniff` command-line utility with the `show` operation:

```
> p3dhcpsniff --show
SCE-Sniffer DHCP LEG:
=====
Active:      true
DHCP message types:
             DHCPACK
             DHCPRELEASE
DHCP options with package information:
             type = 43, subtype = 102
             type = 43, subtype = 101
Subscriber ID:
             Option:    82:2
             Format:    binary
             Fallback: none
Command terminated successfully
>
```

## Viewing the SCE-Sniffer DHCP LEG Statistics

The following is an example of using the `p3dhcpsniff` command line utility with the `show-statistics` operation:

```
> p3dhcpsniff --show-statistics
SCE-Sniffer DHCP LEG statistics
=====
Received DHCP RDRs: 12
RDRS for DHCP initial login or lease renewal: 12
RDRs for DHCP release: 0
Invalid DHCP RDRs: 0
count of DHCP RDRS without option 82: 0
Command terminated successfully
>
```

## Viewing the SCE-Sniffer DHCP LEG Version

The following is an example of using the `p3dhcpsniff` command line utility with the `show-version` operation:

```
> p3dhcpsniff --show-version
SCE-Sniffer DHCP LEG 3.0.5
```



# Index

---

## A

- About the SCMS SM SCE-Sniffer DHCP LEG • 1-1
- Audience • iii

## C

- Cable/Satellite Modem • 3-1
- Cisco.com • vii
- Configuring the General Settings • 1-4
- Configuring the Package Association • 2-4
- Configuring the SCE-Sniffer DHCP LEG • 1-4
- Contacting TAC by Telephone • viii
- Contacting TAC by Using the Cisco TAC Website • vii
- Conventions • iv
- CPE (Customer Premise Equipment) • 3-1

## D

- DHCP ACK packet • 3-1
- DHCP initial login transaction • 1-2
- DHCP initial logon transaction • 3-1
- DHCP lease extension transaction • 2-2
- DHCP lease extension transaction (renewal) • 3-1
- DHCP release transaction • 3-1, 2-2
- DHCP Sniffer • 3-1
- Document Revision History • iii
- Documentation CD-ROM • vi
- Documentation Feedback • vi
- Dynamic Assignment of Package Information • 3-4

## E

- Example • 2-4, 4-4

## I

- Installing the SCE-Sniffer DHCP LEG • 1-3
- Installing the SCE-Sniffer DHCP LEG Module • 1-3

## L

- LEG (Login Event Generator) • 2-1

## O

- Obtaining Documentation • v
- Obtaining Technical Assistance • vi
- Ordering Documentation • vi
- Organization • iv

## P

- p3dhcpsniff Utility • 1-5
- Preface • iii

## R

- RDR (Raw Data Record) • 3-1
- Related Documentation • iv

## S

- SCE-Sniffer DHCP LEG Functionality • 1-2
- Static Assignment of Package Information • 4-4
- Subscriber Domain • 4-1
- Subscriber Mappings • 4-1
- Subscriber Package • 4-1

## T

- Technical Assistance Center • vii
- Terms and Concepts • 2-1
- The SCE-Sniffer DHCP LEG Module • 2-1

**U**

Uninstalling the SCE-Sniffer DHCP LEG •  
2-3

Upgrading the SCE-Sniffer DHCP LEG • -3  
3

Using the SCE-Sniffer DHCP LEG CLU •  
1-5

**V**

Viewing the SCE-Sniffer DHCP LEG  
Statistics • 2-5

Viewing the SCE-Sniffer DHCP LEG Status  
• 2-5

Viewing the SCE-Sniffer DHCP LEG  
Version • 2-5

**W**

World Wide Web • v