Cisco SCMS SM SCE-Sniffer DHCP LEG Reference Guide

Release 3.1
May 2007

Americas 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: 408 527-0883

Customer Order Number:
Text Part Number: OL-8235-04

Cisco SCMS SM SCE-Sniffer DHCP LEG Reference Guide

CONTENTS

About this Guide

Revised: May 30, 2007, OL-8235-04

This document describes the concept of a DHCP Login Event Generator (LEG) based on a DHCP Sniffer, 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, the Cisco SCA BB application, and the DHCP protocol.

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

This introduction provides information about the following topics:

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.

Document Revision History

Cisco Service Control Release	Part Number	Publication Date
Release 3.1.0	OL-8235-04	May, 2007

Description of Changes

- The LEG now supports multiple policies. See Dynamic Assignment of Policy Information.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.5	OL-8235-03	November, 2006

Description of Changes

- Changes in how to dynamically assign package information. See Dynamic Assignment of Policy Information.
- Addition of **is_cable** parameter to the configuration file.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.3	OL-8235-02	May, 2006

Description of Changes

- No major changes or new features in this revision.

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

Description of Changes

- First version of this document.

Organization

The major sections of this guide are as follows:

Table 1

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

Related Publications

Use this *Cisco SCMS SM SCE-Sniffer DHCP LEG Reference Guide* in conjunction with the following Cisco documentation:

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

Document Conventions

This guide uses the following conventions:

- **Bold** is used for commands, keywords, and buttons.
- *Italics* are used for command input for which you supply values.
- `Screen` font is used for examples of information that are displayed on the screen.
- **`Bold screen`** font is used for examples of information that you enter.

- Vertical bars (|) indicate separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({}) indicate a required choice.
- Braces within square brackets ([{}]) indicate a required choice within an optional element.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the guide.

Timesaver Means the *described action saves time*. You can save time by performing the action described in the paragraph.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. To see translated versions of warnings, refer to the *Regulatory Compliance and Safety Information* document that accompanied the device.**

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

CHAPTER 1

About the SCE-Sniffer DHCP LEG

This module describes the Subscriber Manager SCE-Sniffer DHCP LEG software module and the terms and concepts relevant to the SCE-Sniffer DHCP LEG.

Information About the SCE-Sniffer DHCP LEG

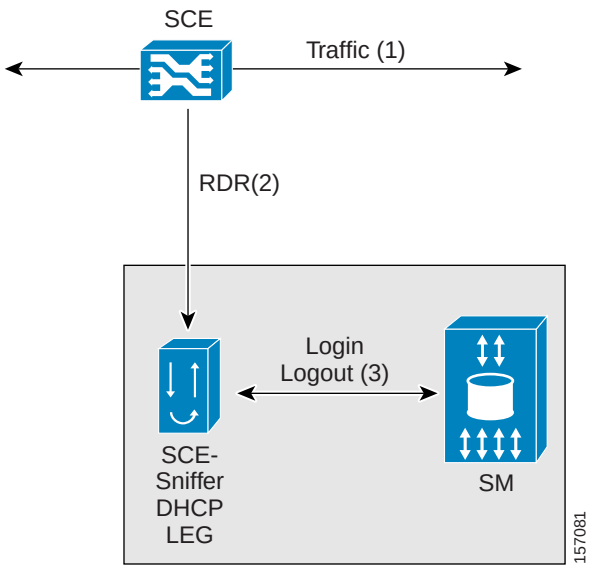
The SCMS SM SCE-Sniffer DHCP LEG is a software module that receives RDR (Raw Data Record) messages containing DHCP information from SCE devices configured with a DHCP sniffer service. The SCE-Sniffer DHCP LEG is an extension of the Subscriber Manager (SM) software and runs as part of the SM.

SCE-Sniffer DHCP LEG Operation

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 logon or logout operation to the SM.

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

Figure 1-1 SCE-Sniffer DHCP LEG Operation



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 *Cisco SCMS Subscriber Manager User Guide* .

- LEG (Login Event Generator)
- RDR (Raw Data Record)
- Cable/Satellite Modem
- CPE (Customer Premise Equipment)
- DHCP ACK Packet
- DHCP Lease Extension Transaction (Renewal)
- DHCP Release Transaction
- DHCP Sniffer
- Subscriber Mappings
- Subscriber Domain
- Subscriber Package

LEG (Login Event Generator)

A software component that performs subscriber login and logout operations on the SM, which 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 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 the "Configuration File Options" section in the *Cisco 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 Policy Association and the *Cisco Service Control Application for Broadband User Guide* .

Information About SCE-Sniffer DHCP LEG Functionality

The SCE devices analyze the DHCP ACK packets of DHCP transactions and send the information to the SCE-Sniffer DHCP LEG that resides on the SM. The LEG performs login and 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 logon , lease extension , and release .

- DHCP Initial Logon Transaction
- DHCP Lease Extension Transaction
- DHCP Release Transaction

DHCP Initial Logon Transaction

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

- Subscriber ID

  For cable environments—The subscriber ID is the modem MAC address, which you extract 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 contains the modem MAC address in the DHCP initial logon transaction. If option 82 is missing, it is not possible to perform a logon operation. Furthermore, the value of option 82 is compared with the **haddr** field to identify modem transactions and not login the modem IP address to the SM.

  For non-cable DHCP environments—The LEG supports using other DHCP options for the subscriber ID. If the DHCP option does not exist in the packet, it is possible to use the IP address as a fallback. In this case, the subscriber ID is in the format IP_a.b.c.d.

The chain of decisions regarding the subscriber-ID is as follows:

1. Use the configured DHCP option as the subscriber-ID if it exists.
2. Otherwise, if the fallback to IP is enabled, use the IP address.
3. Otherwise, attempt to extend the lease based solely on the IP address. (This will only work if the IP address is in the database).

- 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 address* in the DHCP message.

  If the transaction correlates to a CPE device, the assigned IP address for that CPE device 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 logon 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 logon operation is performed.

- Policy

  The policy 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 packet does not contain package information, 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 logon operation to the SM.

DHCP Lease Extension Transaction

The same attributes are extracted from the DHCP lease extension transaction as for the DHCP initial logon 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 to the other DHCP transactions. If the transaction correlates to a CPE device, the LEG performs an SM logout operation with the IP address of the CPE, which appears as a released IP address in the packet itself.

Note A logout operation is also performed when the lease time of the subscriber is expired, and the SM is configured to perform auto logouts. Release transactions also trigger logout operations, but do not replace the auto logout mechanism of the SM.

CHAPTER 2

Installing the SCE-Sniffer DHCP LEG

This module describes the procedures for installing, uninstalling, and upgrading the SCE-Sniffer DHCP LEG on the SM.

How to Install, Uninstall, and Upgrade the SCE-Sniffer DHCP LEG

This module describes the procedures for installing, uninstalling, and upgrading the SCE-Sniffer DHCP LEG on the SM.

The SCE-Sniffer DHCP LEG is 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.

- Installing the SCE-Sniffer DHCP LEG
- Uninstalling the SCE-Sniffer DHCP LEG
- Upgrading the SCE-Sniffer DHCP LEG

Installing the SCE-Sniffer DHCP LEG

Prerequisites

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 *Cisco Service Control Application for Broadband User Guide* .

SUMMARY STEPS

1. Install the PQI file of the SCE-Sniffer DHCP LEG
2. Run the **p3inst** command-line utility (CLU) from the SM CLU directory **~pcube/sm/server/bin**
3. Edit the SCE-Sniffer DHCP LEG configuration files.
4. Load the configuration files to the SM using the **p3sm**CLU

5. Configure the SCE to send RDRs to the LEG

DETAILED STEPS

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

a. Run the **p3inst**command-line utility (CLU) from the SM CLU directory **~pcube/sm/server/bin**

Example:

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

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

Step 2 Edit the SCE-Sniffer DHCP LEG configuration files.

The SCE-Sniffer DHCP LEG includes two configuration files under **~pcube/sm/server/root/config** :

- **dhcpsnif.cfg** —Configures general attributes of the LEG
- **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 for more information.

Step 3 Load the configuration files to the SM using the **p3sm**CLU

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

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

Example:

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

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. You must 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 following CLI.

```
SCE2000>configureSCE2000(config)>RDR-formatter destinationSM-IPportportcategory number 3
priority 100SCE2000(config)>exit
```

Uninstalling the SCE-Sniffer DHCP LEG

SUMMARY STEPS

1. Remove the configuration of the RDR-formatter.

2. Uninstall the SCE-Sniffer DHCP LEG by running the **p3inst**CLU

DETAILED STEPS

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>configureSCE2000(config)>no RDR-formatter
destinationSM-IPportportSCE2000(config)>exit
```

Step 2 Uninstall the SCE-Sniffer DHCP LEG by running the **p3inst**CLU

Example:

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

Note After the uninstall process, the SM restarts automatically.

Upgrading the SCE-Sniffer DHCP LEG

The SCE-Sniffer DHCP LEG and SM versions must be identical; therefore, the SCE-Sniffer DHCP LEG must be upgraded as part of the SM upgrade process. The upgrade for the SCE-Sniffer DHCP LEG should be performed together with the upgrade process of the SM.

SUMMARY STEPS

1. Backup the configuration files of the SCE-Sniffer DHCP LEG.
2. Force the SCEs to store the RDRs during the upgrade.
3. Uninstall the SCE-Sniffer DHCP LEG by running the **p3inst** CLU
4. Perform an upgrade of the SM
5. Install the new version of the SCE-Sniffer DHCP LEG by running the **p3inst**CLU
6. Restore the configuration files of the SCE-Sniffer DHCP LEG.
7. To make the SCEs send the RDRs that they stored during the upgrade, enable the RDR Server on the SM by setting the start parameter in the RDR Server section to true.
8. Load the new configuration of the SM by running the **p3sm** CLU

DETAILED STEPS

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 Force the SCEs to store the RDRs during the upgrade.

To force the SCEs to store the RDRs, disable the RDR Server on the SM by setting the **start** parameter in the RDR Server section to **false**and loading the configuration by running the following CLU:

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

Step 3 Uninstall the SCE-Sniffer DHCP LEG by running the **p3inst** CLU

Example:

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

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

Step 4 Perform an upgrade of the SM

The SM upgrade procedure is described in the *Cisco SCMS Subscriber Manager User Guide* .

Step 5 Install the new version of the SCE-Sniffer DHCP LEG by running the **p3inst**CLU

Example:

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

Step 6 Restore the configuration files of the SCE-Sniffer DHCP LEG.

Step 7 To make the SCEs send the RDRs that they stored during the upgrade, enable the RDR Server on the SM by setting the start parameter in the RDR Server section to true.

Step 8 Load the new configuration of the SM by running the **p3sm** CLU

Example:

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

CHAPTER 3

Configuring the SCE-Sniffer DHCP LEG

This module describes how to configure the SCE-Sniffer DHCP LEG.

Information About Configuring the SCE-Sniffer DHCP LEG

The SCE-Sniffer DHCP LEG is configured using two configuration files, **dhcpsnif.cfg** and **dhcp_pkg.cfg** , which reside 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 resides in **dhcpsnif.cfg**. The dynamic package association configuration resides in **dhcp_pkg.cfg**.

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 runs 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 all login operations should use the default domain “subscribers”.

  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 *Cisco SCMS Subscriber Manager User Guide* .

- `is_cable`

  Indicates whether to check if this is a cable modem transaction; i.e., compare the value of the Remote-Id sub-option (option 82 sub-option 2) with the **haddr** DHCP header field. If it is a cable modem transaction, use only the policy information.

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

The **[Sniffer]** section contains the following parameters:

- `packet_types`

  Contains the DHCP packet types to send 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, use the configuration file to enable the RDR server in the SM.

The **[Subscriber ID]** section contains the following parameters:

- `dhcp_option`

  Defines which DHCP option to use for subscriber ID association. For DHCP options that have sub options, a colon separates the DHCP option and the sub option. The default value is Relay-Agent-Information using the Remote-Id information, i.e. **82:2**.

- `dhcp_option_type`

  Defines the format type of the DHCP option defined by the **dhcp_option** parameter above.

  Possible values for this parameter are **binary**or **string**. The default value is **binary**.

- `default_id`

  Defines the type of fallback that occurs when packet does not contain the configured DHCP option.

  The possible value for this parameter is **ip**for using the allocated IP to create a subscriber ID in the format IP_a.b.c.d. If this parameter is not set, no fallback occurs, and the login fails. The default is not set.

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
is_cable=true
[Sniffer]
packet_types=DHCPACK
[Subscriber ID]
```

```
dhcp_option=82:2
dhcp_option_type=binary
default_id=ip
```

Configuring Policy Association

Note The configuration described in this section is optional.

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

- Dynamic assignment of policy information using information extracted from the DHCP packet, See Dynamic Assignment of Policy Information.
- Static assignment of a constant package Id for all subscribers that log on via the SCE-Sniffer DHCP LEG, See Static Assignment of Policy Information.
- Dynamic Assignment of Policy Information
- Dynamic Assignment of Policy Information Example
- Static Assignment of Policy Information

Dynamic Assignment of Policy Information

Dynamic assignment of policy information is supported if the policy information is submitted in the DHCP packets. The LEG concatenates the desired options and creates a policy-name . It is possible to map, using the configuration, between the policy-names and the application policy parameters such as package IDs and Virtual-links. The SCE-Sniffer DHCP LEG can support multiple policies.

To extract the policy information data from the DHCP packet, use the **dhcp_pkg.cfg** configuration file to define the option types that contain the policy information and define the conversion map of the policy-names to the package IDs (or any other policy) of the Service Control Application for Broadband (SCA BB).

The LEG is able to add additional data to the login operation based on the LEG configuration. This data is added as a key-value pair. Other modules in the login chain can use this data, such as the SOAP LEG (see the *Cisco SCMS SM SOAP LEG Reference Guide*). This data can be created by concatenating the data of several DHCP options and can be given a user-defined label.

The **[DHCP.Policy.XXX]** sections contain the following parameters:

- `options_order_for_policy_name`

  Defines the DHCP options that contain the policy association information and defines the order of concatenation of the data. The DHCP header field called giaddr (Relay-Agent IP) is also supported; it requires the use of the type integer in the **option_type** parameter.

  This parameter has no default value.

  The format is: **option[:subtype],option[:subtype],giaddr**

- `options_type`

  Defines the format type of the DHCP options and fields defined by the **options_order_for_policy_name** parameter.

Possible values for this parameter are **binary**(a binary string that is converted to an ASCII hexadecimal string), **string**(an ASCII string), or **integer**(a 4-byte integer converted to an IP address string in dotted notation). Order the list in the same way as **options_order_for_policy_name**.

This parameter has no default value.

- `name_seperator_value`

  Defines the separator character to use between two options when concatenating them to each other to create the policy name. Any character is accepted. The default value is '_'.

- `use_default`

  Determines whether to use a default policy when no policy information can be extracted from the DHCP data, such as the configurable options are missing or no options were configured.

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

- `default_policy`

  Defines the default policy ID to use if no policy information is extracted from the DHCP data. This parameter is relevant only if the **use_default** parameter is set to **true**.

  Possible values for this parameter are any integer number. This parameter has no default value.

- `allow_login_with_no_policy`

  Defines whether to perform a login without policy information when no policy 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 for this parameter are **true**or **false**. The default value is **true**.

- `policy_property_name`

  Defines the name of the application property that contains the policy information. This parameter has no default value.

- `log_all`

  Defines whether to write detailed user-log messages for all policy association events.

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

- `log_default_assignment`

  Defines whether to write a user-log message for every assignment of the default value (as defined by the **default_policy** parameter).

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

- `mapping_table.<policy_name>`

  Multiple entries containing the information to convert from the policy information as it appears in the DHCP packet to the policy property value to be used by the SCA BB application.

  These entries do not have default values.

The **[Additional Data]** section of the configuration file contains the following parameters:

- `label_options`

  Defines which DHCP option to extract to add to the login operation.

  Possible values are the option number or, in the case of DHCP options with sub-options, the option and sub-option separated by a colon. For example, 43:123 or 61.

  There is no default value for this parameter.

- `label_keys`

  Defines the keys that should mark the DHCP options defined by the **label_options** parameter.

  There is no default value for this parameter.

- `label_options_type`

  Defines the format type of the DHCP option defined by the **label_options** parameter.

  Possible values for this parameter are **binary**(a binary string that is converted to an ASCII hexadecimal string) or **string**(an ASCII string).

  The default value is **binary**.

Dynamic Assignment of Policy Information Example

Suppose that the policy information appears inside option 43 (Vendor Specific Option) of the DHCP packet and that both subtypes, 102 and 101, are in use. Configure the **options_order_for_policy_name** parameter as follows:

```
options_order_for_policy_name=43:102,43:101
```

Suppose that option 43 with subtype 102 contains the type of package (gold, silver, or bronze), and that 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, configure the mapping_table entries as follows:

```
mapping_table.gold_domain1=11
mapping_table.gold_domain2=12
mapping_table.silver_domain1=13
mapping_table.silver_domain2=14
```

This configuration means 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, the package ID that will be associated to the subscriber in the SM will have the value 11.

The following configuration describes how to add the data of the Relay-Agent Circuit-Id option as additional data to the login operation:

```
[Additional Data]
label_options=82:1
label_keys=PORT_ID
label_option_type=string
```

The following is an example of the entire configuration file:

```
[DHCP.Policy.Package]
options_order_for_policy_name=43:102,43:101
name_separator_value=_
use_default=true
default_policy=1
policy_property_name=packageId
allow_login_with_no_policy=false
log_all=false
log_default_assignment=false
mapping_table.gold_domain1=11
mapping_table.gold_domain2=12
mapping_table.silver_domain1=13
mapping_table.silver_domain2=14
[Additional Data]
label_options=82:1
label_keys=PORT_ID
label_option_type=string
```

Static Assignment of Policy Information

If the installation does not require dynamic assignment of package information, the configuration file **dhcp_pkg.cfg** should define the default package ID to be assigned to all the subscribers, as shown in the following example:

```
[DHCP.Policy.Package]
policy_property_name=packageId
allow_login_with_no_policy=false
use_default=true
default_policy=1
[DHCP.Policy.VirtualLinkDownstream]
policy_property_name=downVlinkId
allow_login_with_no_policy=false
use_default=true
default_policy=0
[DHCP.Policy.VirtualLinkUpstream]
policy_property_name=upVlinkId
allow_login_with_no_policy=false
use_default=true
default_policy=0
```

All other configuration parameters should not be set.

CHAPTER 4

Using the SCE-Sniffer DHCP LEG CLU

This module describes the SCE-Sniffer DHCP LEG CLU.

Information About the SCE-Sniffer DHCP LEG CLU

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

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

Table 4-1 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 --showSCE-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-statisticsSCE-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
Number of DHCP RDRs without subscriber Id: 0
Failed logins: 0
Failed logouts: 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-versionSCE-Sniffer DHCP LEG 3.1.0 Build 176
>
```