SCMS SM RDR DHCP LEG Reference Guide

OL-7202-01

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-138632=
Text Part Number: OL-7202-01

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. T his 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 ORIMPLIED, 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 INABILTY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, 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, CCIE, 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, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R)

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

SCMS SM RDR DHCP LEG *Reference Guide*

CONTENTS

Preface iii

Audience iii

Technical Support iv

Cisco TAC Website iv

Opening a TAC Case iv

TAC Case Priority Definitions iv

About the SCMS SM RDR DHCP LEG 1-1

Terms and Concepts 1-2

LEG (Login Event Generator) 1-2

RDR (Raw Data Record) 1-2

CM\SM (Cable\Satellite Modem) 1-2

CPE (Customer Premise Equipment) 1-2

DHCP ACK packet 1-2

DHCP initial logon transaction 1-2

DHCP lease extension transaction (renewal) 1-2

DHCP release transaction 1-3

DHCP Sniffer 1-3

Subscriber Mappings 1-3

Subscriber Domain 1-3

Subscriber Package 1-3

RDR DHCP LEG Functionality 2-1

DHCP initial login transaction 2-1

DHCP lease extension transaction 2-2

DHCP release transaction 2-2

Installing the RDR DHCP LEG 3-1

Installation Procedure Overview 3-1

Installation Procedure 3-2

Uninstalling the RDR DHCP LEG 3-3

Configuration 4-1

General Configuration 4-1

Example 4-2

Package Association Configuration 4-3

Dynamic Assignment of Package Information 4-3

Static Assignment of Package Information 4-4

RDR DHCP LEG CLU 5-1

p3rdr Utility 5-1

RDR Server Status 5-1

RDR Server Statistics 5-2

RDR Server Connections 5-2

p3rdrdhcp Utility 5-2

RDR DHCP LEG Status 5-3

RDR DHCP LEG Statistics 5-3

Index 1

Preface

This document briefly 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 subscriber management, subscriber integration concepts, and the DHCP protocol

For complete information regarding Cisco's subscriber integration concept, see the *Service Control Management Suite, Subscriber Manager (SCMS SM) User Guide*

Audience

This document is intended for readers that are familiar with the RDR DHCP LEG concepts and with Cisco Service Control Subscriber Management and Subscriber Integration concepts.

The following typographic conventions are used in this guide:

Typeface or Symbol	Meaning
Italics	References, new terms, field names, and placeholders.
Bold	Names of menus, options, and command buttons.
`Courier`	System output shown on the computer screen.
`Courier Bold`	CLU command code typed in by the user in examples.
`Courier Italic`	Required parameters for CLU commands.
`[italic in brackets]`	Optional parameters for CLU commands.
➲	A one-step procedure.
✎	Note. Notes contain important information.
⚠	Warning. Warning means danger of bodily injury or of damage to equipment.

Technical Support

Cisco TAC Website

The Cisco TAC website (*http://www.cisco.com/tac* (http://www.cisco.com/tac)) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL: *http://tools.cisco.com/RPF/register/register.do* (http://tools.cisco.com/RPF/register/register.do)

Opening a TAC Case

The online TAC Case Open Tool (*http://www. cisco.com/tac/caseopen* (http://www.cisco.com/tac/caseopen)) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution.

If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer. For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL: *http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml* (http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml)

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

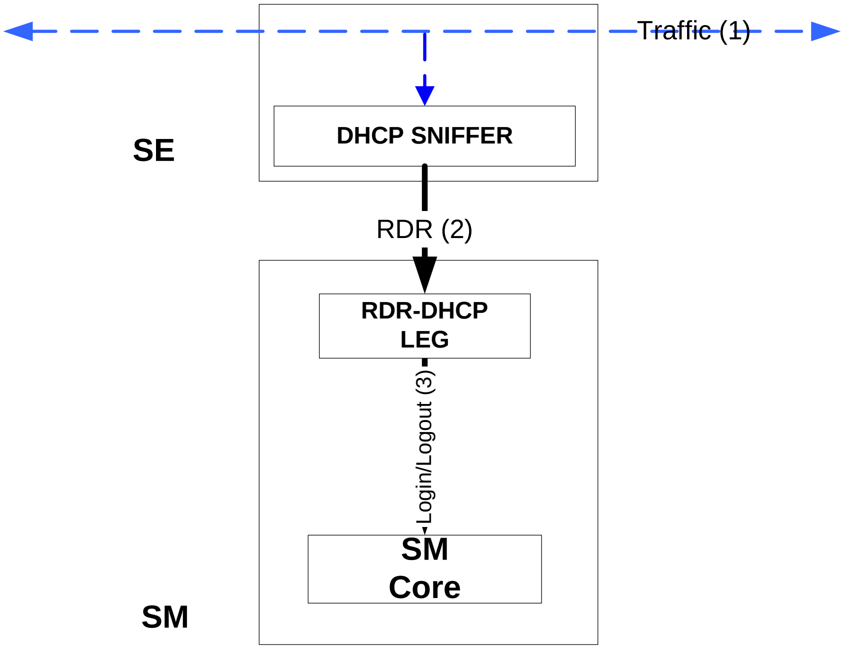
CHAPTER 1

About the SCMS SM RDR DHCP LEG

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

The SCE device analyzes DHCP traffic, and reports the DCHP 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.

Following is a sequence diagram representing the operation of the LEG:



This chapter contains the following sections:

- Terms and Concepts 1-2

Terms and Concepts

The following is a list of some terms and concepts that are necessary to understand the RDR DHCP LEG and SM configuration and operation. Additional information regarding the various issues can be found in the *Service Control Management Suite Subscriber Manager (SCMS SM) User Guide*.

LEG (Login Event Generator)

A software component that performs subscriber login and logout operations on the SM, that 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.

CM\SM (Cable\Satellite Modem)

A data modem that provides Internet access over Cable \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 its 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 DHCPACK packet, the results of the transaction are final. This packet is the only packet that is analyzed by the RDR DHCP LEG by default. It is possible to configure the LEG to analyze additional packets as well.

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. Since the modem is used as the subscriber name, it is required that the modem MAC address will added by the DHCP relay agent during initial logon query using option 82.

DHCP lease extension transaction (renewal)

A DHCP transaction for renewal of the entity's lease time. When the lease time is 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 the subscriber from the SM.

DHCP Sniffer

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

Subscriber Mappings

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

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.

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 CLU.

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

Subscriber Package

The policy enforced by Cisco solutions on a certain subscriber is usually defined by a policy package. The RDR 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
- Leave the package ID unset.

For additional information, see *Package Association Configuration* (on page 4-3), and the *User's Guide* of the *Cisco Service Control Application Suite* for *Broadband* application.

CHAPTER 2

RDR DHCP LEG Functionality

The SCE devices analyze the DHCP ACK packets of DHCP transactions, and send the information to the LEG that resides in the SM. 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

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 (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. Note that 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. Note that option 51 must contain the lease time, otherwise no login is performed.

- 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. In case 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

Note: In order to handle release transactions, it is required to configure the LEG to handle DHCP Release packets as well (by default the LEG only handles DHCP Ack packets)

CHAPTER 3

Installing the RDR DHCP LEG

This section describes the procedures for configuring and running the RDR DHCP LEG. It also describes the uninstall procedure.

The RDR DHCP LEG is provided as an external component (PQI file) of the SM software that should be installed separately using the SM command line utilities. THE RDR DHCP LEG distribution is part of the SM CD.

The installation package of the LEG includes a set of configuration files and command line utilities for the LEG.

This chapter contains the following sections:

- Installation Procedure Overview 3-1
- Installation Procedure 3-2
- Uninstalling the RDR DHCP LEG 3-3

Installation Procedure Overview

Following is a general overview of the RDR DHCP LEG installation procedure. Refer to the relevant sections for specific instructions.

To install the RDR DHCP LEG:

Step 1 Verify that the SCAS for Broadband application is installed on all the SM and SCE devices. If not, install the application as described in the SCAS for Broadband User Manual.

Step 2 Install the PQI file of the RDR DHCP LEG. See Install the PQI file of the RDR DHCP LEG below.

Edit the configuration files of the RDR DHCP LEG. See Edit the configuration files of the RDR DHCP LEG below.

Load the configuration files to the SM using the command line utilities. See Load the configuration files to the SM below.

Configure the SCE to send RDRs to the LEG. See Configure the SCE to send RDRs to the LEG below.

Configure the SCE to listen to DHCP traffic, and generate reports accordingly. See Configure the SCE to listen to DHCP traffic below.

Installation Procedure

Note **Note:** After the installation of the PQI file, the SM restarts itself automatically.

To Install the RDR DHCP LEG:

Step 1 Install the PQI file of the RDR 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 rdrdhcp.pqi
```

Step 2 Edit the configuration files of the RDR DHCP LEG

The RDR DHCP LEG includes 2 configuration files:

a) p3rdr_dhcp.cfg - configures general attributes of the LEG

b) p3dhcp_pkg.cfg - configures rules for package assignment

It is recommended to familiarize yourself with these files immediately after the first installation, and edit them according to your specific needs. See the *Configuration* (on page 4-1) chapter for more information.

Step 3 Load the configuration files to the SM

Step 4 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 5 Configure the SCE to send RDRs to the LEG

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

```
SCE2000> configure
SCE2000(config)> RDR-formatter destination <SM-IP> port 33001
category number 3 priority 100
SCE2000(config)> exit
```

Step 6 Configure the SCE to listen to DHCP traffic

a) Run the SCAS for Broadband Console application which is included in the SCAS distribution. (See the SCAS for Boradband User Guide for detailed instructions for installing and using the SCAS Console).

b) Add a new service to the configuration, and name it *DHCP Service*.

c) Open the Prototocl setting window (Configuration è Protocols)

d) Delete the port based protocols *bootps* and *bootpc*.

e) Locate the signature-based protocol DHCP Sniff, and add UDP ports 67 & 68 to it.

f) Add a service element to the *DHCP Service*, using the *DHCP Sniff* protocol, and configure the initiating side to "Initiated by either side".

g) Apply the new service configuration to the SCE device that is supposed to serve as the DHCP sniffer.

Note

Note: In order support SM cluster topology, set the cluster VIP as the SM-IP in the CLI above.

Uninstalling the RDR DHCP LEG

To uninstall the RDR DHCP LEG:

Step 1 Configure the SCE to stop listening to the DHCP traffic:

a) Run the SCAS for Broadband Console application which is included in the SCAS Distribution. (See the SCAS for Boradband User Guide for detailed instructions for installing and using the Console).

Remove the DHCP Service from the configuration.

Apply the new service configuration to the SCE device that is supposed to serve as the DHCP sniffer.

Step 2 Configure the SCE to stop sending RDRs to the LEG

Run the RDR-formatter CLI in the SCE to remove the LEG as category 3 RDR destination

```
SCE2000> configure
SCE2000(config)> no RDR-formatter destination <SM-IP> port 33001
SCE2000(config)> exit
```

Step 3 Uninstall the RDR DHCP LEG:

Step 4 Run the p3inst command line utility from the SM CLU:

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

Note

Note: After the uninstall process, the SM restarts itself automatically.

CHAPTER 4

Configuration

The RDR DHCP LEG is configured using 2 configuration file **p3rdr_dhcp.cfg**, and **p3dhcp_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 are built of sections that are defined by brackets; 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 this is a remark line.

General configuration of the RDR DHCP LEG and the RDR server resides in **p3rdr_dhcp.cfg**. Configuration regarding dynamic package association resides in **p3dhcp_pkg.cfg.**

This chapter contains the following sections:

- General Configuration 4-1
- Package Association Configuration 4-3

General Configuration

Following is a description of the configuration variables of **p3rdr_dhcp.cfg**.

The `[RDR Server]` section contains the following parameters:

- **start**
  Defines whether the SM should run the RDR server at startup.
  Possible values for this parameter are `yes` and `no`. The default value is `no`.
  To receive the DHCP messages from the SCE, this parameter must be set to `yes`.

- **port**
  Defines the RDR server's port number.
  The default value is `33001`.

Note

Note: To control the IP addresses that are allowed to connect to this port configure an access control list on the machine.

- **max_connections**
  Defines the maximum number of connections that can be accepted by the server.
  The default value is `10`.

The [RDR-DHCP-LEG] section contains the following parameters:

- **start**
  Defines whether the SM should run the RDR 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`.
  Note that the RDR server must be activated as well for the RDR DHCP LEG to function correctly.
- **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 which is 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 SM 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:
  `DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, DHCPNACK, DHCPRELEASE`.
  The default value is set to `DHCPACK`.

Example

Following is a sample of a configuration file:

```
[RDR Server]
start=yes
port=33001
max_connections=10

[RDR-DHCP-LEG]
start=yes
log_failures=true
log_all=false
use_default_domain=true

[Sniffer]
packet_types=DHCPACK
```

Package Association Configuration

Note **Note:** The configuration described in this section is optional.

Subscriber package configuration in the RDR 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 RDR 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's package-Ids.

To extract the package information data from the DHCP package the configuration file **p3dhcp_pkg.cfg** should define the option types that contain the package information, and the conversion map of *package names* to the package IDs of SCAS.

The `[Package Association]` section contains the following parameters:

- **options_order_for_package_name**
  Defines the DHCP options (the option's format must be strings) that contain the package association information, and defines the order of concatenation of these option data.
  The format is `option[:subtype],option[:subtype]`
- **name_seperator_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 is '_'
- **use_default**
  Determines whether a default package should be used when no package information can be extracted from the DHCP data. (in case 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 is set to `true`.
  Possible values are each 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 use_default is set to false.
  This parameter is relevant only if use_default 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. Default value is `packageId`, as used by SCAS.

The `[Package Names]` section contains the conversion information of the package information as appears in the DHCP packet to the package ID number to be used by the SCAS for Broadband application.

Example

Suppose that the package information appears inside option 43 (Vendor Specific Option) of the DHCP packet, and suppose that both subtypes 102 and 101 are in use. Then 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 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, the package names should be configured as follows (for example):

```
[Package Names]
gold_domain1=11
gold_domain2=12
silver_domain1=13
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, then the package ID that will be associated to the subscriber in the SM will have the value 11.

An example of the entire configuration file follows:

```
[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 **p3dhcp_pkg.cfg** should define the default package Id to be assigned to all the subscribers, as the following sample:

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

All the other configuration parameters should not be set.

CHAPTER 5

RDR DHCP LEG CLU

This chapter contains the following sections:

- p3rdr Utility 5-1
- p3rdrdhcp Utility 5-2

p3rdr Utility

The **p3rdr** utility is used for viewing the RDR server configuration and statistics. Command format: `p3rdr <OPERATION>`The following tables list the **p3rdr** operations and options.

Table 5-1 p3radius Operations

Operation	Description
--show	Displays the RDR server configuration, as well as other general info (maximum connections, etc.)
--show-statistics	Displays counters of RDR messages handled or failed for each connection
--show-connections	Displays a list of active connections

The user of the RDR DHCP LEG can use the `p3rdr` command line utility to view the RDR Server's status and statistics.

RDR Server Status

Following is an example using the `p3rdr` command line utility with the `show` operation:

```
> p3rdr --show
Active:    true
Port:      33001
Connections:
        Max-limit: 10 connections
        Current:   2 connections
Command terminated successfully
>
```

RDR Server Statistics

Following is an example of using the p3rdr command line utility with the show-statistics operation:

```
> p3rdr --show-statistics
RDR Server Statistics:
======================
Handled RDRs: 12
Bad RDRs:     0
Current rate: 12.0 RDRs per second
Peak rate:    12.0 RDRs per second
Client statistics:
-----------------:
Connection from 10.1.8.81 statistics:
        Handled RDRs:    7
        Bad RDRs:        0
        Current rate:    7.0
        Is connected:    true
        Times connected: 1
Connection from 10.1.8.82 statistics:
        Handled RDRs:    5
        Bad RDRs:        0
        Current rate:    5.0
        Is connected:    true
        Times connected: 1
Command terminated successfully
>
```

RDR Server Connections

Following is an example of using the p3rdr command line utility with the show-connections operation:

```
> p3radius --show-connections
The following clients are connected:
10.1.8.81 - 1 connection
10.1.8.82 - 1 connection
Command terminated successfully
>
```

p3rdrdhcp Utility

The **p3rdrdhcp** utility is used for viewing RDR DHCP LEG configuration and statistics. Command format: p3rdrdhcp <OPERATION>The following tables list the **p3rdrdhcp** operations and options.

Table 5-2 p3rdrdhcp Operations

Operation	Description
--show	Displays all of RDR DHCP LEG configurations and status
--show-statistics	Displays counters of DHCP messages handled and number of logon operations performed

The user of the RDR DHCP LEG can use the p3rdrdhcp command line utility to view the RDR DHCP LEG's status and statistics.

RDR DHCP LEG Status

Following is an example using the `p3rdrdhcp` command line utility with the `show` operation:

```
> p3rdrdhcp --show
RDR DHCP LEG:
============
Active:    true
DHCP message types:
        DHCPACK
DHCP options with package information:
        type = 43, subtype = 102
        type = 43, subtype = 101
Command terminated successfully
>
```

RDR DHCP LEG Statistics

Following is an example of using the `p3rdrdhcp` command line utility with the `show-statistics` operation:

```
> p3rdrdhcp --show-statistics
DHCP RDR 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
>
```

Index

A

About the SCMS SM RDR DHCP LEG • 1-1
Audience • iii

C

Cisco TAC Website • iv
CM\SM (Cable\Satellite Modem) • 1-2
Configuration • 4-1
CPE (Customer Premise Equipment) • 1-2

D

DHCP ACK packet • 1-2
DHCP initial login transaction • 2-1
DHCP initial logon transaction • 1-2
DHCP lease extension transaction • 2-2
DHCP lease extension transaction (renewal) • 1-2
DHCP release transaction • 1-3, 2-2
DHCP Sniffer • 1-3
Dynamic Assignment of Package Information • 4-3

E

Example • 4-2, 4-4

G

General Configuration • 4-1

I

Installation Procedure • 3-2
Installation Procedure Overview • 3-1
Installing the RDR DHCP LEG • 3-1

L

LEG (Login Event Generator) • 1-2

O

Opening a TAC Case • iv

P

p3inst Utility • 5-1, 5-2
p3rdr Utility • 5-1
p3rdrdhcp Utility • 5-2
Package Association Configuration • 4-3
Preface • iii

R

RDR (Raw Data Record) • 1-2
RDR DHCP LEG CLU • 5-1
RDR DHCP LEG Functionality • 2-1
RDR DHCP LEG Statistics • 5-3
RDR DHCP LEG Status • 5-3
RDR Server Connections • 5-2
RDR Server Statistics • 5-2
RDR Server Status • 5-1

S

Static Assignment of Package Information • 4-4
Subscriber Domain • 1-3
Subscriber Mappings • 1-3
Subscriber Package • 1-3

T

TAC Case Priority Definitions • iv
Technical Support • iv
Terms and Concepts • 1-2

U

Uninstalling the RDR DHCP LEG • 3-3