



SCMS SM CNR LEG Reference Guide

OL-7201-01

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-138631=
Text Part Number: OL-7201-01



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, 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 CNR LEG Reference Guide

Copyright © 2002-2005 Cisco Systems, Inc.
All rights reserved.



Preface iii

Audience iii

Document Conventions iii

Technical Support iv

 Cisco TAC Website iv

 Opening a TAC Case iv

 TAC Case Priority Definitions iv

About the CNR LEG 1-1

Terms and Concepts 1-1

 Subscriber Mappings 1-2

 Subscriber Domain 1-2

 RPC Protocol (PRPC) 1-2

 Subscriber Mode 1-2

 SM Cable Support Module 1-2

 SM C++ API 1-3

 Communication Link Failure Handling 1-3

 Subscriber Auto-logout 1-3

Getting Started 2-1

Prerequisites 2-1

Package Contents 2-1

Installation 3-1

Installation Procedure Overview 3-1

Windows Installation 3-1

Solaris Installation 3-2

Uninstalling the CNR LEG 3-3

 Uninstall Procedure Overview 3-4

 Uninstall Procedure 3-4

Configuration 4-1

CNR LEG Configuration 4-1

SM IP Address and Port 4-1

Subscriber Mode 4-2

Lease Time Option 4-2

SM Configuration 4-2

SM-LEG Failure Handling Configuration 4-3

SM-LEG Failure Handling 4-3

LEG-Domains Association 4-4

Domain Aliases 4-4

Auto-logout 4-5

PRPC Server Configuration 4-6

CNR LEG Functional Specification A-1

CNR LEG High Level Design A-1

Logging and Tracing A-2

Extensions Point Operation A-2

init-entry A-2

post-send-packet A-3

post-packet-decode A-3

Index 1



Preface

This document explains how to install and configure the Cisco Network Registrar (CNR) Login Event Generator (LEG) on Solaris and Windows NT/2000 platforms.

Audience

This document is intended for readers that are familiar with the CNR extensions concept and with Cisco Service Control Subscriber Management and Subscriber Integration concepts.

Document Conventions

The following typographic conventions are used in this guide:

Typeface or Symbol	Meaning
<i>Italics</i>	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.
<i>Courier Italic</i>	Required parameters for CLU commands.
[<i>italic in brackets</i>]	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.



About the CNR LEG

The CNR LEG is a software module that forwards login/logout events from CNR to the Cisco Service Control Management Suite. The CNR LEG is actually a CNR extension developed in C++. The extension points used by CNR LEG are:

- `init-entry`
- `post-send-packet`
- `post-packet-decode`

The CNR requires the use of option 82 (CM-MAC) in all DHCP requests including in renewal transactions. If no option 82 (CM-MAC) exists in a renewal transaction an attempt to extend the lease based solely on the IP address is performed, this will succeed only if this IP address was previously logged-in to the SM by the LEG (in an event of a full DHCP transaction) or via other interfaces of the SM

For additional information about extending the CNR functionality using extension points, see the *Service Control Management Suite CNR CLI Reference Guide*.

The CNR LEG works with the SM's cable support module, and supports only the “CPE as Subscriber” mode. For additional information about cable environment subscriber modes, see *Appendix A* of the *Service Control Management Suite (SM) User Guide*.

CNR LEG was carefully developed and thoroughly tested on Solaris and Windows platforms for both functional correctness and robustness. It does not jeopardize the stability or the reliability of the CNR.

This chapter contains the following sections:

- [Terms and Concepts](#) 1-1

Terms and Concepts

This section defines terms and concepts that are necessary for understanding the CNR and Subscriber Management (SM) configuration and operation. More information about all items can be found in the *Service Control Management Suite (SM) User Guide*.

Subscriber Mappings

The main function of the CNR 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. (For information about the SCE Platforms, see the *SCE1000* and *SCE2000 User Guides*) 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 SM configuration file and can be viewed using the SM CLU.

It is also possible to configure domain aliases. A domain alias is a synonym for the actual domain name in the SM. Domain aliases are configured in the SM configuration file.

For additional information about domains and domain aliases, see *Chapter 5* and *Appendix A* of the *Service Control Management Suite (SM) User Guide*.

RPC Protocol (PRPC)

The CNR LEG communicates with the SM using a proprietary RPC (PRPC) protocol developed by Cisco. PRPC is also used by the SM Java, C, and C++ APIs. The CNR LEG uses the C++ API as its communication layer.

Subscriber Mode

The Subscriber Mode defines which entity is referred to as the subscriber in the LEG and in the SM.

Cable providers usually prefer using the Cable Modem (CM) as the subscriber entity to be assigned multiple IP addresses (one per CPE). Previous implementations of the CNR LEG did not support such functionality (CM as a subscriber entity).

The CNR LEG supports the modes *CPE as Subscriber* and *CM as Subscriber* (the default), as defined by the configuration.

SM Cable Support Module

The cable support module is an SM component that exposes an API that is friendly to cable environment integrations. The cable support module is a translator between the cable world subscriber terminology (CPE, CM, CMTS) and the generic subscriber terms used by the Cisco Service Control Management system. The CNR LEG uses PRPC to invoke the `cableLogin` and `cableLogout` operations that are exposed by the cable support module API.

The SM cable support module is used only in the *CPE as Subscriber* mode.

For additional information about the cable support module, see the *Service Control Management Suite (SM) User Guide, Appendix C*.

SM C++ API

The SM C++ API exposes a set of operations designed to enable subscriber integration with the Cisco system. The CNR LEG uses the SM C++ API as its basic communication layer.

For additional information about the C++ API, see the *Service Control Management Suite (SM) C/C++ API User Guide*.

Communication Link Failure Handling

The communication link (socket) between the CNR LEG and the SM is periodically checked using a keep-alive mechanism. The communication link fails when the socket is closed or a keep-alive timeout occurs. The keep-alive timeout can be configured in the SM configuration file.

In cases where LEG-SM link fails, the SM can be configured to clear the mappings of all the subscribers that are updated by the failed LEG.

To learn more about the communication link failure handling, see Chapter 6 and *Appendix A* of the *Service Control Management Suite (SM) User Guide*.

Subscriber Auto-logout

The SM supports the configuration of an auto-logout timer for each subscriber. The timer can be set when a subscriber `cableLogin` operation is performed. The CNR LEG can extract and set an auto-logout value from the DHCP IP lease expiration time option.

Package Contents

Root	Folder (under root)	File name	Notes
		asn1ber.dll	
		asn1rt.dll	
		cnrleg.dll	



Note The directory in which the CNR is installed is referred to as `cnr-inst-dir`



Installation

This chapter describes the procedures for installing the CNR LEG on both Windows and Solaris platforms. It also describes the uninstall procedure.

This chapter contains the following sections:

- [Installation Procedure Overview](#) 3-1
- [Windows Installation](#) 3-1
- [Solaris Installation](#) 3-2
- [Uninstalling the CNR LEG](#) 3-3

Installation Procedure Overview

Following is a general overview of the CNR LEG installation procedure. Refer to the relevant sections for specific instructions for your platform.

To install the CNR LEG:

-
- Step 1** Extract the CNR LEG package tar file and copy the distribution files matching your OS to the appropriate location. (See the appropriate installation section: *Windows Installation* (on page [3-1](#)) or *Solaris Installation* (on page [3-2](#))).
 - Step 2** Edit the CNR configuration file. (See *CNR LEG Configuration* (on page [4-1](#))).
 - Step 3** Verify that the SM is configured correctly. (See *SM Configuration* (on page [4-2](#))).
 - Step 4** Register the CNR LEG using the CNR `nr cmd` command line utility. (See the appropriate installation section: *Windows Installation* (on page [3-1](#)) or *Solaris Installation* (on page [3-2](#))).
-

Windows Installation

- Step 1** Extract the distribution and copy the files:

Unzip the CNR Package to `pkg-ext-dir`.

Copy all files under `pkg-ext-dir\winnt` to `cnr-inst-dir\Extensions\DHCP\Dex\`.

Copy the sample configuration file from `pkg-ext-dir\doc` to a directory of your choice, hereafter referred to as `cfg-dir`.

Step 2 Configure the CNR LEG:

Edit the sample configuration file. See *CNR LEG Configuration* (on page 4-1).

Step 3 Configure the SM:

Configure the SM. See *SM Configuration* (on page 4-2).

Step 4 Register the CNR LEG with CNR:

Run the CNR `nrcmd` command line utility.

Log in.

Configure the following:

```
nrcmd> extension smleg create dex cnrleg.dll cnrLegPostSendPacket
nrcmd> extension smleg set init-entry=cnrLegInitEntry
nrcmd> extension smleg set init-args=cfg-dir/cnrleg.cfg
nrcmd> dhcp attachExtension post-send-packet smleg 1
nrcmd> extension smlegext create dex cnrleg.dll
cnrLegPostPacketDecode
nrcmd> dhcp attachExtension post-packet-decode smlegext 1
nrcmd> save
nrcmd> server DHCP reload
```



Note You must use the `cfg-dir` full path as the `init-args` argument.



Note You must use a slash (“/”) and not a back-slash (“\”) as the path separator.

Solaris Installation

Step 1 Extract the distribution and copy the files:

Extract the CNR Package to `pkg-ext-dir`; for example:

```
#> tar xvf cnr-leg-vvv.bb.tar
```

The abbreviations `vvv` and `bb` stand for the CNR LEG version and build number.

Copy `libcnrleg.so` under `pkg-ext-dir/solaris` to `cnr-inst-dir/extensions/dhcp/dex`.

Copy the sample configuration file from `pkg-ext-dir/doc` to a directory of your choice, hereafter referred to as `cfg-dir`.

Step 2 Configure the CNR LEG:

Edit the sample configuration file. See *CNR LEG Configuration* (on page 4-1).

Step 3 Configure the SM:

Configure the SM. See *SM Configuration* (on page 4-2).

Step 4 Register the CNR LEG with CNR:

Run the CNR `nrcmd` command line utility.

Log in.

Configure the following:

```
nrcmd> extension smleg create dex libcnrleg.so cnrLegPostSendPacket
nrcmd> extension smleg set init-entry=cnrLegInitEntry
nrcmd> extension smleg set init-args=cfg-dir/cnrleg.cfg
nrcmd> dhcp attachExtension post-send-packet smleg 1
nrcmd> extension smlegext create dex libcnrleg.so cnrLegPostPacketDecode
nrcmd> dhcp attachExtension post-packet-decode smlegext 1
nrcmd> save
nrcmd> server DHCP reload
```



Note You must use the `cfg-dir` full path as the `init-args` argument.



Note You must use a slash (“/”) and not a back-slash (“\”) as the path separator.

Uninstalling the CNR LEG

This section explains how to uninstall the CNR LEG. The uninstall procedure is the same on both Windows and Solaris platforms.

Uninstall Procedure Overview

-
- Step 1** To uninstall the CNR LEG:
- a) Un-register CNR LEG from CNR.
 - b) *(Optional)* Delete the LEG distribution files.
-

Uninstall Procedure

This procedure is applicable to both Windows and Solaris platforms.

-
- Step 1** To un-register CNR LEG from CNR:
Run the CNR `nrcmd` command line utility.

Log in.

Configure the following:

```
nrcmd> dhcp detachExtension post-send-packet 1
nrcmd> extension smleg delete
nrcmd> dhcp detachExtension post-packet-decode 1
nrcmd> extension smlegext delete
nrcmd> save
nrcmd> server DHCP reload
```

- Step 2** To delete the LEG distribution files:

This part of the uninstall procedure is optional.

Delete all files copied to `cnr-inst-dir/extensions/dhcp/dex`

Delete the configuration file (`<cfg-dir>/cnrleg.cfg`).



Configuration

This chapter contains the following sections:

- [CNR LEG Configuration 4-1](#)
- [SM Configuration 4-2](#)

CNR LEG Configuration

The CNR configuration file offers the following configuration options to the user:

- SM IP address - the IP address of the SM
- SM port - the TCP port to which the SM PRPC server listens
- Subscriber mode - the subscriber entity to be used by the LEG: CM as subscriber (default) or CPE as subscriber.
- Lease time option - the DHCP option number from which to extract the lease expiration time that is to be sent to the SM

SM IP Address and Port

You must set the SM IP address correctly in order for the LEG to operate.

The default PRPC TCP port number generally does not need to be changed.

The SM port default is 14374. The SM PRPC port can be retrieved from the SM configuration file. For additional information, see *Appendix A* of the *Service Control Management Suite (SM) User Guide*.

Example

Following is a portion of a sample CNR configuration file showing how to configure the SM IP address and port:

```
[sm]
# SM IP address
ip_address= 216.239.37.99
# SM PRPC Server port. default 14374
#port=14374
```

Subscriber Mode

The LEG can operate in one of two modes:

- CM as Subscriber - each CPE login/logout/lease extension triggers a logon operation to the SM using the corresponding CM MAC as the subscriber ID.
- CPE as Subscriber - each CPE is a subscriber entity in and of itself. Each CPE login/logout/lease extension triggers a logon operation to the SM using both the CPE MAC and the CM MAC as the subscriber ID.

Example

Following is a portion of a sample CNR configuration file showing how to configure the Subscriber Mode:

- CM as Subscriber:

```
[general]
# defines who is the subscriber to refer to the CM or the CPE.
# default: cm_as_subscriber optional values: cm_as_subscriber \
# cpe_as_subscriber
subscriber_mode=cm_as_subscriber
```

- CPE as Subscriber:

```
[general]
# defines who is the subscriber to refer to the CM or the CPE.
# default: cm_as_subscriber optional values: cm_as_subscriber \
# cpe_as_subscriber
subscriber_mode=cpe_as_subscriber
```

Lease Time Option

In order to enable subscriber auto-logout at lease time expiration on the SM, the `lease_time` option must be set. The CNR LEG can extract the IP address lease expiration from one of the following DHCP option numbers:

- 51 (default)
- 58
- 59

For additional information about auto-logout mechanism see *Auto-logout* (on page 4-5).

Example

Following is a portion of a sample CNR configuration file showing how to configure the lease time option:

```
lease_time_option=51
```

SM Configuration

The SM is configured using the SM configuration file. For additional information, see *Appendix A* of the *Service Control Management Suite (SM) User Guide*.

SM-LEG Failure Handling Configuration



Note It is **important** to properly configure the SM-LEG failure handling on the SM. In the *Service Control Management Suite (SM) User Guide*, see the *Communication Failures* section of *Chapter 3* as well as *Appendix A*.

In order to activate the failure handling, you must edit the following sections of the configuration file:

- SM-LEG Failure Handling
- LEG-Domains association

SM-LEG Failure Handling

By default, SM-LEG failure handling is **not** activated. In order to activate SM-LEG failure handling, you must do the following:

- Set the `clear_all_mappings` parameter to `true`.
- (optional) Change the `timeout` value.

Example

Following is a portion of a sample `p3sm.cfg` configuration file showing how to configure SM-LEG failure handling:

```
[SM-LEG Failure Handling]
# The following parameter defines the behavior of the SM in case of
# LEG-SM connection failure.
# This parameter is relevant only for cases SM and LEG are running on
# different machines.
# Note that this parameter defines a behavior that is similar for ALL
# connected LEGs. If the parameter is set to true then in case of
# LEG-SM connection failure that is not recovered within the defined
# timeout, the mappings of all subscribers in the domains
# defined in the 'LEG-Domains Association' section for the LEG that
# was disconnected, will be removed
#
# IMPORTANT: LEG Domains must be defined in the following section in
# case this parameter is set to 'true'
#
# Optional values: [true/false]. Default: false.

clear_all_mappings=true

# The following parameter defines the time in seconds from a LEG-SM
# connection failure until clearing the mappings in the SM database.
# Default value: 60.

timeout=60
```

LEG-Domains Association

You must set LEG-Domains associations in order for the SM-LEG failure handling to work. The CNR-LEG name to be used in this section is a concatenation of the hostname of the machine on which the LEG is installed and the suffix ".CNR.LEG".

An alternate way to retrieve the CNR-LEG name is by using the **p3rpc** utility. This utility displays all clients currently connected to the PRPC server, including the CNR.

Step 1 To retrieve the CNR-LEG name by using the p3rpc utility:

- At the prompt, type:

```
> p3rpc -show-client-names
```

Example

If the hostname of the machine on which the LEG is installed is `netserv5`, then the LEG name to be used in the configuration file is `"netserv5.CNR.LEG"`. The following example assumes that the subscriber domain associated with the CNR LEG is named `subscribers`.

Following is a portion of a sample `p3sm.cfg` configuration file showing how to set LEG-Domains associations.

```
[LEG-Domains Association]
# The following parameter defines domains that the mapping of all
# subscribers that belong to them will be cleared on LEG-SM connection
# failure. The key is the LEG NAME and the value is a comma separated
# list of domain names.
# A value of * in domain names stands for all the subscriber domains
# in the system.
# A value of * in LEG name means all the LEGs that are connected to
# the SM
# LEG NAME1 = domain_name1, domain_name2
# LEG NAME2 = domain_name2, domain_name3

netserv5.CNR.LEG=subscribers
```

Domain Aliases

You must set domain aliases in order for the CNR LEG to operate correctly.

The CNR LEG uses the CMTS IP for the subscriber domain name. You should make sure that all the CMTS IP addresses appear as an alias to exactly one subscriber domain. Domain aliases are configured in the SM configuration file.



Note

You do **not** have to configure domain aliases in those cases where each CMTS updates a single subscriber domain *and* you have configured the subscriber domain names in the SM to be the IP address of the matching CMTS.

Example

In this example the SM is configured as follows:

- A single subscriber domain named `subscribers`

- Four CMTS devices with the following IP addresses:
 - 209.247.228.201
 - 209.247.228.202
 - 69.42.72.147
 - 69.42.72.148

Following is a portion of a sample `p3sm.cfg` configuration file showing how to configure the domain aliases.

```
[Domain.subscribers]

# The following parameter defines domain aliases. When subscriber
# information is received
# from the LEG with certain alias the information will be distributed
# to the domain that matches this alias - domain that contains this
# alias in its aliases list.
#
# A typical alias could be a network device IP address. For example,
# each string in the values can be the IP address of a NAS or a CMTS.
#
# In order to distribute all subscriber operations on all unmapped
# domains to a certain domain use aliases=*. Note that only one domain #
# section may include this alias.

aliases=209.247.228.201,209.247.228.202,69.42.72.147,69.42.72.148
```

Auto-logout

If you want subscribers to be automatically logged out when their lease expires, you should configure the SM auto-logout interval. After every “auto-logout interval” time, the SM checks which subscriber IP addresses have a lease time that has expired, and begins to automatically remove these IP addresses from the system.

Lease time is the timeout defined by the LEG during the login operation per each IP address, based on the Lease-Time option. All subscriber login events will start a timer of `lease_time` seconds. When the timer expires (and the `grace_period`, see below, has also passed), the subscriber's IP-addresses are removed (causing the subscriber to be removed from the SCE Platform's database). Note that any login event by the subscriber with an existing IP address during the timer countdown period resets the timer, causing it to restart.

If the interval value is set to zero (0), the SM's auto-logout mechanism is disabled.

If the interval is set to a value greater than zero, the SM's auto-logout mechanism is enabled.



Note

Note that the subscriber record (with no mappings) remains in the SM database, preserving the subscriber state.

Example

Following is a portion of a sample `p3sm.cfg` configuration file showing how to configure the auto-logout interval to 60 minutes:

```
[Auto Logout]

# The following parameter configures the time between each run of the
# auto-logout mechanism. After every "auto-logout" time interval, the SM
# checks which subscriber IP addresses have a lease time that has expired,
# and begins to automatically remove these IP addresses from the system
# (causing it to be removed from the SCE platform's database).

# Auto-logout should be activated when the LEG/API can't provide
# logout indications.

auto_logout_interval=3600

# The following parameter defines the grace period in seconds for subscriber
# auto logout. A subscriber will be logged out only after timeout period +
# grace period seconds.

grace_period=10

# The following parameter defines the maximum rate (logouts per second) that
# the auto-logout task will perform logouts from the system. this enables to
# spread the load of the logout operations over time, and reduce the
# performance impact on other operations. the value should be calculated so
# it spreads the logouts over at least half of 'auto_logout_interval' time.
# (default 50)

max_rate=50
```

PRPC Server Configuration

In order for the CNR LEG to be able to communicate with the SM, the PRPC server must be up and running. The RPC server is started by default, therefore it does not require special configuration.

Following is a portion of a sample `p3sm.cfg` configuration file showing the PRPC server configuration:

```
[RPC.Server]

# RPC server port (default 14374)

port=14374
```

Step 1 To view the status of the PRPC server in the SM:

- At the prompt, type:

```
> p3rpc --show
```



CNR LEG Functional Specification

This appendix describes the CNR LEG design, logging, and tracing, as well as the operations performed by the LEG in each extension point. The purpose of this appendix is to provide insight into the CNR LEG operation and integration with CNR.

CNR LEG High Level Design

The CNR LEG uses extension points:

- `init-entry`
- `post-packet-decode`
- `post-send-packet`

When an extension point hook is called, the following sequence of events takes place:

-
- Step 1** The extension point hook performs the minimal computation necessary to extract all the required data and calls a Non-blocking C++ API operation.
 - Step 2** The non-blocking operation encodes a message and places it in a queue.
 - Step 3** The Non-blocking C++ API network task reads messages from the message buffer and sends them over the network to the PRPC Server on the SM.
 - Step 4** The PRPC Server decodes the message and passes it to the cable support module, which sets up the subscribers in the SM database using the SM core functionality.

- Reading the configuration file
- Initializing the LEG logging and tracing
- Creating a Non-blocking C++ API instance and connecting it to the SM
- Starting the C++ API network-task thread
- Termination:
 - Stopping and freeing the Non-blocking C++ API instance
 - Stopping the C++ API network-task thread

post-send-packet

The extension point `post-send-packet` is used for sending `cableLogin` operations to the SM:

- Verifying that the request-dictionary is for DHCP REQUEST and the response dictionary is for DHCP ACK
- Extracting CM-MAC, CPE-MAC, and CMTS-IP from the request dictionary
- Extracting the assigned CPE-IP and lease time from the response dictionary
- Calling the Non-blocking C++ API `cableLogin` operation with the parameters extracted
- In case there is no CM-MAC (option 82) an attempt to extend the lease based solely on the IP address is performed

post-packet-decode

The extension point `post-packet-decode` is used for sending `cableLogout` operations to the SM:

- Verifying that the request dictionary is for either DHCP RELEASE or DHCP DECLINE
- Extracting CM-MAC, CPE-MAC, CPE-IP, and CMTS-IP from the request dictionary
- Calling the Non-blocking C++ API `cableLogout` operation with the parameters extracted



Index

A

About the CNR LEG • 1-1
Audience • iii
Auto-logout • 4-5

C

Cisco TAC Website • iv
CNR LEG Configuration • 4-1
CNR LEG Functional Specification • A-1
CNR LEG High Level Design • A-1
Communication Link Failure Handling • 1-3
Configuration • 4-1

D

Document Conventions • iii
Domain Aliases • 4-4

E

Example • 4-1, 4-2, 4-3, 4-4, 4-6
Extensions Point Operation • A-2

G

Getting Started • 2-1

I

init-entry • A-2
Installation • 3-1
Installation Procedure Overview • 3-1

L

Lease Time Option • 4-2
LEG-Domains Association • 4-4
Logging and Tracing • A-2

O

Opening a TAC Case • iv

P

Package Contents • 2-1
post-packet-decode • A-3
post-send-packet • A-3
Preface • iii
Prerequisites • 2-1
PRPC Server Configuration • 4-6

R

RPC Protocol (PRPC) • 1-2

S

SM C++ API • 1-3
SM Cable Support Module • 1-2
SM Configuration • 4-2
SM IP Address and Port • 4-1
SM-LEG Failure Handling • 4-3
SM-LEG Failure Handling Configuration • 4-3
Solaris Installation • 3-2
Subscriber Auto-logout • 1-3
Subscriber Domain • 1-2
Subscriber Mappings • 1-2
Subscriber Mode • 1-2, 4-2

T

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

U

Uninstall Procedure • 3-4
Uninstall Procedure Overview • 3-4
Uninstalling the CNR LEG • 3-3

W

Windows Installation • 3-1

