



Cisco RFSS Network Controller User Guide

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

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 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 NON-INFRINGEMENT 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Cisco RFSS Network Controller User Guide

Copyright © 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

Audience v

Organization v

Obtaining Documentation, Obtaining Support, and Security Guidelines vi

CHAPTER 1

Introduction 1-1

Network Controller Description 1-1

Platform Requirements 1-2

Hardware 1-2

Software 1-3

CHAPTER 2

Interfaces 2-1

RNC Interfaces 2-1

RNC to NLR Interface 2-1

RNC to Sites in the Local RFSS Interface 2-1

RNC to Other RFSS Interface 2-2

User Indications and RNC Logging 2-2

CHAPTER 3

Configuration 3-1

Gathering Information 3-1

Configuring the System Host File 3-2

Updating the RNC Configuration File 3-3

RNC Global Parameters 3-3

SIP Stack Parameters 3-6

NLR Parameters 3-7

Media Controller Parameters 3-8

RTP Stack Parameters 3-10

String Definitions 3-10

Configuring the NLR for Home RFSS Information 3-10

Configuring the System Watchdog 3-12

Configuring SNMP for Fault Management 3-13

Configuring NTP 3-14

RNC Application 3-15

Starting and Stopping the RNC Using the Watchdog 3-15
Manually Running the RNC 3-16
SNMP Alarms and Alerts 3-16

CHAPTER 4

Troubleshooting 4-1

The RNC Fails to Start 4-1
The RNC Displays a "Could Not Create Sip Stack" Error 4-1
The RNC Fails to Find Entries in "Rnc.config" 4-2
The RNC Cannot Communicate With the NLR 4-2
The RNC Cannot Communicate With Entities Other Than the NLR 4-3
The "monit" Command Reports a Duplicate 4-3
The RPM Package Installation Hangs 4-4
The SNMP Manager Does not Receive Alarms or Alerts 4-4

GLOSSARY

INDEX



Preface

This document provides a description of the functionality of the Cisco RFSS Network Controller (RNC), including details of its primary characteristics, and how to install, configure, and use this application.

Audience

This document is intended for users and developers who are required to deploy or work with the Cisco RFSS Network Controller. It is assumed that you have a working knowledge of the following:

- Radio technology.
- APCO P25 standards.
- The operating system used by the RFSS Network Controller and associated applications.
- The core network functionality of Cisco.

Organization

This document is organized as follows:

Chapter 1, “Introduction”	Introduces the main functions of the RFSS Network Controller, as well as system hardware and operating system requirements.
Chapter 2, “Interfaces”	Describes aspects of the Network Controller, including network interfaces, event logs, and hardware and network status indicators.
Chapter 3, “Configuration”	Provides information about how to configure the RFSS Network Controller.
Chapter 4, “Troubleshooting”	Describes some of the most common problems that may need to be resolved to get the RNC operating correctly following a new installation, configuration, or upgrade.

**Note**

This user guide does not cover every application and configuration of the RFSS Network Controller and the troubleshooting section describes only some of the most common problems that may be encountered during the deployment of the system.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and 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

Introduction

The P25 RFSS Network Controller (RNC) is the central controller for a Radio Frequency Subsystem (RFSS) and provides all mobility and call management between other network entities within the RFSS. It interacts with the Network Location Register (NLR) to facilitate updates to and queries about subscriber units and group members. It also provides APCO P25 ISSI capabilities to enable wide area calls to other RFSSs within a P25 wide area system.

The NLR stores data about subscribers and groups operating within a single RFSS. It can function as a traditional Home Location Register (HLR) for an APCO P25 system as well as a Visitor Location Register (VLR) for roaming subscribers, that is, those subscribers that are not declared ("homed") at this RFSS. For more information about the NLR, see the Cisco Network Location Register Series User Guide.

Network Controller Description

The RNC consists of a Commercial Off-The-Shelf (COTS) PC and can be co-hosted on the same machine as an NLR, depending upon the specific requirements of the installation. All interfaces are IP based so no special cables or hardware are required.

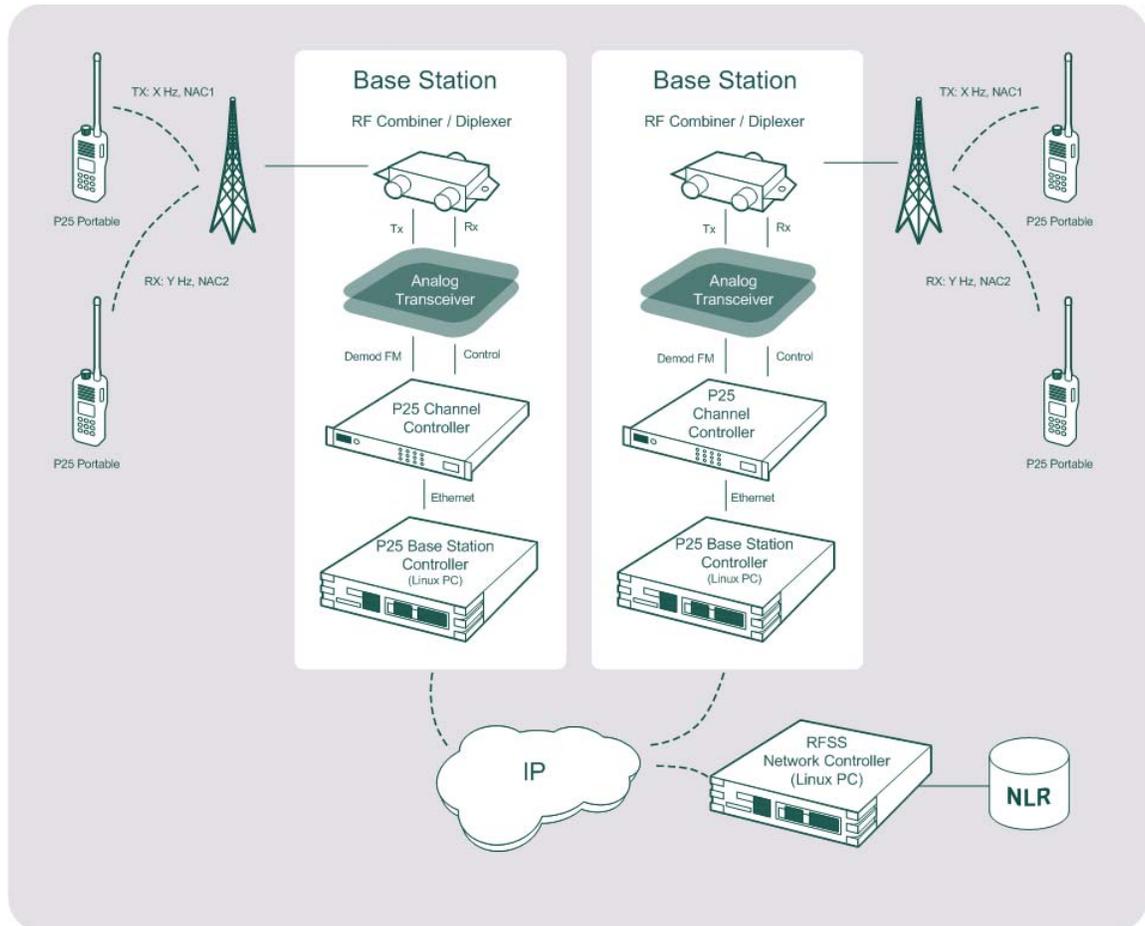
The RNC also communicates with the NLR to look up subscriber and group profile information, as well as updating current mobile location. Together, the RNC and NLR manage the subscriber units that are within their home system as well as providing visitor services to subscriber units which are homed at another P25 System (or RFSS) but are roaming within this RFSS.

The RNC includes a Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) stack for communicating with base station sites within its RFSS as well as to other RFSSs. The RFSS interfaces to other RFSSs via the Inter-RF Sub System Interface (ISSI) interface.

The RNC is not a standard SIP network element but uses SIP and RTP with APCO P25 specific extensions required for delivering individual and group calls across the core network. These P25 specific extensions are based on the ISSI interface.

[Figure 1-1](#) shows an example of a multiple RFSS, consisting of one or more base stations and a central RFSS Network Controller along with the NLR. Other possible network elements in the local RFSS can include Soft Radios (SRs), Public Switched Telephone Network (PSTN) gateways, Network Management Systems (NMS), Digital Voice Recorders (DVRs) and console applications.

Figure 1-1 Typical Multi Site RFSS



Platform Requirements

Hardware

The RNC requires no special equipment to install, as it is a software application that runs on any Commercial Off the Shelf (COTS) PC. The RNC will usually plug directly into a local network switch for its network interface. If the RNC is co-hosted with the NLR, it is possible to share a single physical network connection by allocating the primary IP for the RNC and assigning a second virtual IP interface for the Network Interface Function (NIF) process.

Specific hardware requirements are based on system architecture as well as envisaged load, that is, subscriber population and distribution, and calling patterns.

Table 1-1 shows minimum and recommended hardware requirements for some of the more important hardware items. Although it may be possible to use other types of hardware, only the recommended hardware listed in column three (below) has undergone testing.

Table 1-1 Hardware Requirements

Hardware	Minimum Requirement	Recommended
Processor	Pentium 4	Pentium 4
Hard drive(s)	Single drive > 70 GB	Two x 74 GB SATA (RAID 1)
Network Interface Card	One (100 Mb/s)	Three (1 Gb/s)

**Note**

[Table 1-1](#) shows a configuration that would include the Fault Tolerant Server Package, where three network interfaces are recommended. However, with this configuration, support will only be provided at the discretion of Cisco, as currently only a configuration with two network interfaces is supported.

Software

The single supported operating system for the RNC is IPICS OS 4.5. Cisco provides an installer that installs the ISSI Gateway software on IPICS OS. The RNC is included on that software installation.



CHAPTER 2

Interfaces

This chapter describes the RFSS Network Controller (RNC) interfaces, and includes the following sections:

- [RNC Interfaces, page 2-1](#)
- [User Indications and RNC Logging, page 2-2](#)

RNC Interfaces

The RNC has the following three main interfaces:

- [RNC to NLR Interface, page 2-1](#)
- [RNC to Sites in the Local RFSS Interface, page 2-1](#)
- [RNC to Other RFSS Interface, page 2-2](#)

RNC to NLR Interface

The RNC communicates with the NLR (Network Location Register) via an IP-based interface. The RNC uses this interface to access profiles for subscribers and groups homed at that Radio Frequency Subsystem (RFSS). This interface is also used to update and retrieve visiting subscriber information for mobiles that are roaming within this RFSS.

RNC to Sites in the Local RFSS Interface

The RNC interfaces to network elements within the local RFSS. These can include:

- BSCs (Base Station Controllers).
- Soft radios.
- PSTN gateways.
- Network management systems.
- Digital voice recorders.
- Console applications.

This interface is based upon an extension of APCO P25 ISSI standards with SIP (Session Initiation Protocol) and RTP (Real-time Transport Protocol) based protocols to provide the functionality required for sites within the local RFSS. While this interface is not defined in the P25 standards, it is a well defined interface which is used to extend the ISSI in the local RFSS to enable further control of local sites.

RNC to Other RFSS Interface

The interface between the RNC and other RFSSs is defined in the APCO P25 ISSI suite of standards.



Note

Consoles that support the full CSSI effectively appear to the RNC as another RFSS interface.

User Indications and RNC Logging

The RNC normally runs on a Commercial Off the Shelf (COTS) PC, so status indications are provided by the hardware used, that is, power, hard disk and network activity status. If more detailed information is required about the RNC's operation, its log can be consulted. To quickly check recent events, a shell script is provided from the directory /home/RncUser. To do this, execute the following command:

```
bin/tail_ latest.sh log/Rnc.log
```

Logs are stored in the directory /home/RncUser/log. The RNC writes its logging output to the file Rnc.log. The RNC log is rotated on a daily basis into a date-stamped file of the form Rnc.log.YYYYMMDD. For example, the file Rnc.log.20081127 would contain the log for 11/27/2008. By default, log files are held for a maximum of 30 days before being removed.

Within each file, log messages accumulate from all the functional modules of the RNC. Each entry is marked with a label to indicate the part of the RNC from which it originated, along with an indication of its importance on a scale of zero to four, as shown in [Table 2-1](#).

Error! Reference source not found. lists.

[Table 2-1](#) describes the log entry ratings list.

Table 2-1 Log Entry Ratings List

Index	Description
0	Exceptional messages/critical errors
1	Warnings and abnormal program operation
2	Normal operation
3	Verbose output; trivial messages
4	Debug output; most basic level of operation

Time and date-stamp information is also included in each log entry, resulting in output of the following format:

```
YYYY-MM-DD HH:MM:SS.mmm CATEGORY(Level) <Log Message>
```

Where:

YYYY is the year

MM is the date (01 = Jan, 12 = Dec)

DD is the day of month (01 to 31)

HH is the hour of day (00 to 23)

MM is the minute (00 to 59)

SS is the second (00 to 59)

mmm is the millisecond

An example of this output in an actual log file is shown below:

```
2008-11-18 12:36:27.264 RNCC(0) Version - Rnc: 02.04.000 RELEASE
```




CHAPTER 3

Configuration

Once the RFSS Network Controller (RNC) package has been successfully installed, it must be configured to make it fully functional for use as an RFSS Network Controller for all sites. This chapter describes the configuration parameters and steps required to ensure proper RNC functionality, and it includes the following topics:

- [Gathering Information, page 3-1](#)
- [Configuring the System Host File, page 3-2](#)
- [Updating the RNC Configuration File, page 3-3](#)
- [Configuring the NLR for Home RFSS Information, page 3-10](#)
- [Configuring the System Watchdog, page 3-12](#)
- [Configuring SNMP for Fault Management, page 3-13](#)
- [Configuring NTP, page 3-14](#)
- [RNC Application, page 3-15](#)
- [SNMP Alarms and Alerts, page 3-16](#)

Gathering Information

Before configuring the RNC, the following information must be known about how the local RFSS is going to behave and interact with other sites, other RFSSs, and other systems:

- The RFSS identity of the RFSS to which the RNC belongs.
- The System identity of the RFSS to which the RNC belongs.
- The WACN identity of the RFSS to which the RNC belongs.
- NLR configuration details, including database host, name, username and password.
- The site identity and IP address for every site within the RFSS.
- The RFSS identity and IP address of every other RFSS that the RNC may have to communicate with.
- The ranges of Subscriber Unit ID (SUID) and Subscriber Group ID (SGID) that are homed at each RFSS that is known to the RNC.

Configuring the System Host File

To allow the RNC to communicate with other entities, the `/etc/hosts` file must be edited to add an entry for every site within the RFSS that is controlled by this RNC, as well as every other RFSS the RNC is required to communicate with. In addition, there should also be an entry for the RNC itself.

Each entry takes the form of the host's IP address in ABNF quad notation followed by the fully qualified address of the RFSS or the site.

The format of a site address (in ABNF quad notation) is:

```
<Site_Id>".<Rfss_Id>".<System_Id>".<Wacn_Id>".p25dr"
```

The format of an RFSS identity is:

```
<Rfss_Id>".<System_Id>".<Wacn_Id>".p25dr"
```

where `Site_Id`, `Rfss_Id`, `System_Id`, and `Wacn_Id` are ABNF format hexadecimal numbers which are zero padded, the lengths of which are detailed in [Table 3-1](#).

[Table 3-1](#) describes RFSS field lengths.

Table 3-1 RFSS Field Lengths

Field	Length
Site_Id	5 hexadecimal characters (that is, 20 bits)
Rfss_Id	2 hexadecimal characters (that is, 8 bits)
System_Id	3 hexadecimal characters (that is, 12 bits)
Wacn_Id	5 hexadecimal characters (that is, 20 bits)

For example:

The RNC is the controller for RFSS "01" in system "002" and WACN "00003" and has IP address 192.168.1.195.

There are two local BSCs (Base System Controllers) in this RFSS with identities "0B" and "0C" and IP addresses 192.168.1.196 and 192.168.1.197.

The RNC has to be able to communicate with an RFSS with identity "06" and IP address 192.168.1.60 in the same system.

The RNC also has to be able to communicate with RFSS "09" in system "677" and WACN "ABCE" with IP address 192.168.54.2.

The hosts file would appear as shown below:

```
# The RNC
192.168.1.19501.002.00003.p25dr

# Sites controlled by the RNC
192.168.1.1960000B.01.002.00003.p25dr
192.168.1.1970000C.01.002.00003.p25dr

# Other RFSS in this System
192.168.1.16006.002.00003.p25dr
```

```
# Other RFSS
192.168.54.209.677.ABCDE.p25dr
```

Updating the RNC Configuration File

When the System Host file has been configured, the next stage is to update the installed Rnc.config file for the RNC. The release package contains an example configuration file "Rnc.config" which must be modified before the application can be started. This file is located in the directory /home/RncUser/config and contains the parameters required for the RNC process to run correctly.

**Note**

All configuration file changes require a restart of the RNC application before the changes can be read in.

The Rnc.config file is split into sections corresponding to the different parts of the RNC application. These sections are:

- [RNC Global Parameters, page 3-3](#)
- [SIP Stack Parameters, page 3-6](#)
- [NLR Parameters, page 3-7](#)
- [Media Controller Parameters, page 3-8](#)
- [RTP Stack Parameters, page 3-10](#)
- [String Definitions, page 3-10](#)

RNC Global Parameters

The RNC uses the following global parameters, all of which have the prefix "RG":

```
"RG.RegistrationPeriod"="3600"
"RG.AllowVisitingSUServiceHomeNotAvail"="true"
"RG.RgLoggingLevel"="NORMAL"
"RG.NumDstLegsConnectedBeforeCallActive"="0"
"RG.LocalPstngValid"="false"
"RG.LocalPstngSiteAddress"="180"
"RG.RfssId"="1"
"RG.SystemId"="2"
"RG.WacnId"="3"
"RG.ActiveCallNoPttTimeout"="30"
"RG.SdEndToEndTimeout"="3800"
"RG.SdCalledHomeTimeout"="3500"
"RG.SdCalledServingTimeout"="3800"
"RG.RespondToPoll"="true"
```

```
"RG.MinRtpPort"="17000"
"RG.MaxRtpPort"="17998"
"RG.CallLegRetryPeriod"="3000"
"RG.SNMPEEnabled"="false"
```

Table 3-2 describes the RNC global parameters.

Table 3-2 RNC Global Parameters

Field	Type	Description	Default
"RG.RegistrationPeriod"	Integer	Time in seconds that registrations remain valid for. Maximum value is 86400 (one day).	"3600"
"RG.AllowVisitingServiceHomeNotAvail"	Boolean	Whether the RNC allows a subscriber that is visiting this RFSS access when the subscriber's home RFSS is not available. Valid values are: "true" to allow visiting subscribers "false" to disallow visiting subscribers	"true"
"RG.RgLoggingLevel"	Boolean	Whether a PSTN Gateway is available to this RNC. Valid values are: "true" PSTN Gateway present "false" no PSTN Gateway	"false"
"RG.LocalPstngSiteAddress"	Integer	Specifies the decimal site address of the PSTN Gateway located at this RFSS. This entry is ignored if "RG.LocalPstngValid" is set to "false".	"180"
"RG.NumDstLegsConnectedBeforeCallActive"	Integer	The number of destination legs that must be successfully set up before the RNC informs the originator of a call that the setup was successful.	"0"
"RG.RfssId"	Integer	The Radio Frequency Sub-System ID for the RFSS that this RNC controls. Minimum value is: 1 (0x01). Maximum value is: 254 (0xFFE).	"1"
"RG.SystemId"	Integer	The system identity that this RFSS belongs to. Minimum value is: 1 (0x001). Maximum value is: 4095 (0xFFE).	"2"
"RG.WacnId"	Integer	The wide area communications network (WACN) identity this RFSS belongs to. Minimum value is: 1 (0x00001). Maximum value is: 1048575 (0xFFFFE).	"3"

Table 3-2 RNC Global Parameters

Field	Type	Description	Default
"RG.ActiveCallNoPttTimeout"	Integer	The time in seconds a call will remain connected whilst no PTT activity is occurring. Maximum value 86400, that is, 1 day.	"30"
"RG.SdEndToEndTimeout"	Integer	The time in milliseconds a supplementary data service will attempt to be delivered for. Minimum value is: 800. Maximum value is: 9800.	"3800"
"RG.SdCalledHomeTimeout"	Integer	The time in milliseconds the RNC acting as the Called Home RFSS waits for responses from the Called Serving RFSS or local site. Minimum value is: 500. Maximum value is: 9500.	"3500"
"RG.SdCalledServingTimeout"	Integer	The time in milliseconds an RNC acting as the Called Serving RFSS waits for Secondary Response from the Called Home RFSS after sending SD Error Response. Minimum value is: 800. Maximum value is: 9800.	"3800"
"RG.RespondToPoll"	Boolean	Whether this entity responds to network polling by sites.  Note Do not change this value.	"true"
"RG.MinRtpPort"	Integer	The minimum RTP port to use for the RTP media part of all calls.	"17000"
"RG.MaxRtpPort"	Integer	The maximum RTP port to use for the RTP media part of all calls.	"17998"
"RG.CallLegRetryPeriod"	Integer	The time interval in milliseconds the RNC will wait for a failed call leg before initiating a new call. The failure can be during call setup or whilst active if heartbeats determine the leg has failed. This setting only applied to group calls.	"3000"
"RG.SNMPEnabled"	Boolean	Determines if the RNC will send fault management alerts and alarms via SNMP.	"false"

SIP Stack Parameters

The following parameters control SIP stack behaviour:

```
"SIP.LocalPort"="5060"
```

```
"SIP.LoggingSipStack"="false"
```

```
"SIP.LoggingSipStackLevel"="NORMAL"
```

```
"SIP.ShutdownThreadWaitMs"="100"
```

```
"SIP.RetransmissionsOn"="true"
```

```
"SIP.NoAckTimeout"="30"
```

```
"SIP.NoResponseTimeout"="30"
```

```
"SIP.LocalIpAddress"="192.168.1.195"
```

Table 3-3 describes the SIP stack parameters.

Table 3-3 SIP Stack Parameters

Field	Type	Description	Default
"SIP.LocalPort"	Integer	The local port for the SIP stack to listen on.  Note Do not change this value.	"5060"
"SIP.LoggingSipStack"	Boolean	Boolean indicating whether or not to log SIP and RTP activity. Valid values are: "true" to log "false" for no logging	"false"
"SIP.LoggingSipStackLevel"	String	The level to log for SIP and RTP stack activity. Valid values in increasing logging level are: "ALWAYS" "IMPORTANT" "NORMAL" "TRIVIAL" "DEBUG"	NORMAL
"SIP.ShutdownThreadWaitMs"	Integer	The number of milliseconds between SIP stack polling to determine if it should shut down.  Note Do not change this value.	"100"

Table 3-3 SIP Stack Parameters

Field	Type	Description	Default
"SIP.RetransmissionsOn"	Boolean	Indicates whether to turn retransmissions ON for SIP messages. Valid values are: "true" to turn ON retransmissions "false" to have no SIP retransmissions  Note Do not change this value.	"true"
"SIP.NoAckTimeout"	Integer	The number of seconds the SIP stack will wait if no SIP ACK message is received for an INVITE transaction where the SIP stack sends a SIP 200 OK message but does not receive any subsequent SIP ACK.	"30"
"SIP.NoResponseTimeout"	Integer	The maximum number of seconds the SIP stack will wait for any response.	"30"
"SIP.LocalIpAddress"	String	The local IP address to use for SIP and RTP signalling.  Note If this is not set to the RNC's IP address the RNC will exit immediately.	192.168.1.195

NLR Parameters

The following parameters control the connectivity of the RNC to the NLR and its NLR operation:

```
"LRIF.LrIfDatabaseName"="nlr"
"LRIF.LrIfDatabaseHost"="192.168.1.12"
"LRIF.LrIfDatabaseUser"="RncUser"
"LRIF.LrIfDatabasePassword"="etherstack"
"LRIF.LrIfMinVisitorWorkingUnitId"="9000000"
"LRIF.LrIfMaxVisitorWorkingUnitId"="9999999"
"LRIF.LrIfMinVisitorWorkingGroupId"="60000"
"LRIF.LrIfMaxVisitorWorkingGroupId"="65535"
"LRIF.LrIfLoggingLevel"="ALWAYS"
```

Table 3-4 describes the NLR parameters.

Table 3-4 NLR Parameters

Field	Type	Description	Default
"LRIF.LrifDatabaseName"	String	The name of the NLR database to connect to.	"nlr"
"LRIF.LrifDatabaseHost"	String	The IP address of the location the NLR is available at. If the NLR is hosted on the same machine as the RNC this should be the same as the RNC IP Address. The value should be a full IP address.	"192.168.1.195"
"LRIF.LrifDatabaseUser"	String	The username the RNC can access the NLR database with.	"root"
"LRIF.LrifDatabasePassword"	String	The password the RNC requires to access the NLR database with.	"ipics45"
"LRIF.LrifMinVisitorWorkingUnitId"	Integer	The minimum working ID that a visiting subscriber will be issued with when registering.	"9000000"
"LRIF.LrifMaxVisitorWorkingUnitId"	Integer	The maximum working ID that a visiting subscriber will be issued with when registering.	"9999999"
"LRIF.LrifMinVisitorWorkingGroupId"	Integer	The minimum working group ID that a subscriber will be issued with when affiliating to a visitor group.	"60000"
"LRIF.LrifMaxVisitorWorkingGroupId"	Integer	The maximum working group ID that a subscriber will be issued with when affiliating to a visitor group.	"65535"
"LRIF.LrifLoggingLevel"	String	The level to log for the LRIF application. Valid values in increasing logging level are: "ALWAYS" "IMPORTANT" "NORMAL" "TRIVIAL" "DEBUG"	"ALWAYS"

Media Controller Parameters

The following parameters define the behaviour of the Media Controller part of the RNC:

```
"MC.LoggingLevel"="ALWAYS"
"MC.GrantedPttNoVoiceTimeout"="500"
"MC.RtpMulticastLoopback"="false"
"MC.UseHeartbeat"="true"
"MC.TearDownCallIfNoHeartbeat"="true"
```

"MC.HeartbeatInterval"="10"

"MC.NumberVoiceFramesPerRtpPacket"="1"

Table 3-5 describes the Media Controller parameters.

Table 3-5 Media Controller Parameters

Field	Type	Description	Default
"MC.LoggingSipStackLevel"	String	The level to log for media controller activity. Valid values in increasing logging level are: "ALERT" "IMPORTANT" "NORMAL" "TRIVIAL" "DEBUG"	"ALWAYS"
"MC.GrantedPttNoVoiceTimeout"	Integer	The length of time in milliseconds that if no voice activity is received the RNC will assume the transmission attempt has been abandoned (sends a PTT Transmit End) and then allow new transmission attempts.	"500"
"MC.RtpMulticastLoopback"	Boolean	Whether the RNC receives RTP traffic it sends to the network. Valid values are: "true" "false"	"false"
"MC.UseHeartbeat"	Boolean	Whether the MC uses heartbeats during an active RTP connection. Valid values are: "true" "false"	"true"
"MC.TearDownCallIfNoHeartbeat"	Boolean	Whether the MC clears a call if no heartbeat is received. Valid values are: "true" "false"	"true"

Table 3-5 Media Controller Parameters

Field	Type	Description	Default
"MC.HeartbeatInterval"	Integer	Period in seconds between sending and receiving heartbeat messages within an RTP stream.	"10"
"MC.NumberVoiceFramesPerRtpPacket"	Integer	Number of voice frames sent in each RTP packet. Valid values are: "1", "2", or "3"	"1"

RTP Stack Parameters

The RTP parameters are shown below:

```
"RTP.LoggingLevel"="ALWAYS"
```

Table 3-6 describes the RTP stack parameters.

Table 3-6 RTP Stack Parameters

Field	Type	Description	Default
"RTP.LoggingSipStackLevel"	String	The level to log for RTP activity. Valid values in increasing logging level are: "ALWAYS" "IMPORTANT" "NORMAL" "TRIVIAL" "DEBUG"	"ALWAYS"

String Definitions

The string definition section of the configuration file, denoted by lines beginning with `..string`, is used to match a numeral string identifier to the text identifier and should never need to be modified. Only the top half of the configuration file should ever need modification.

Configuring the NLR for Home RFSS Information

The web based interface to the NLR can be used to configure "home" RFSS location information. For more information about the NLR, see the Cisco Network Location Register Series User Guide.

When units register or perform group affiliation from sites in the RFSS the RNC needs to know which RFSS the unit or group is homed at so that it can either process the request itself if the entity is homed locally, or forward the request on to the home RFSS of those entities.

Both the RNC and the NLR manage unit and group location information. The NLR is typically (but not necessarily) installed on the same machine as the RNC and the location information is accessed via the web based interface of the NLR. The web based interface of the NLR is located at `http://<ip-address>/nlr` where `<ip-address>` is the IP address of the NLR host machine.

The NLR must be configured so that it contains an entry identifying the home RFSS for every unit that will register and every group that units affiliate to. Each entry takes the form of a mapping of a home RFSS ID to a range of Unit IDs or Group IDs by defining the first ID in the range and the last ID in the range, where the following conditions exist:

- The RFSS ID consists of a WACN ID, System ID and RFSS ID.
- The first ID in the range is either the minimum Unit ID or Group ID.
- The last ID in the range is either the maximum Unit ID or Group ID.

The range can be as small as a single ID, that is, the minimum and maximum ID are identical and equal to the single ID. Alternatively, there may be a single entry covering the whole range of IDs from "000000" to "FFFFFF" for Unit IDs and "0000" to "FFFF" for Group IDs.

An example of a tri-site system is shown below. For detailed instructions on entering values via the NLR web interface, see the Cisco Network Location Register Series User Guide. Where there are three RFSSs:

- SUIDs "00003002000000" to "000030026FFFFFFF" and "00003002700002" to "00003002FFFFFFF" are homed at 01.002.00003.p25dr (a total of 16,777,213 units).
- SUIDs "00003002700000" to "00003002700001" are homed at 02.002.00003.p25dr (a total of 2 units).
- SUIDs "ABCDE667000000" to "ABCDE66FFFFFFF" are homed at 09.667.ABCDE.p25dr (a total of 16,777,215 units).
- SGIDs "000030020000" to "000030027FFF" are homed at 01.002.00003.p25dr (a total of 32767 groups).
- SGIDs "000030028000" to "00003002FFFF" are homed at 02.002.00003.p25dr (a total of 32767 groups).
- SGIDs "ABCDE667A000" to "00003002FFFF" are homed at 09.667.ABCDE.p25dr (a total of 24575 groups).

Figure 3-1 shows the subscriber to home RFSS mapping table for this configuration.

Figure 3-1 Subscriber Range to Home RFSS Mappings Table - Tri-site System

Subscriber Range to Home RFSS Mappings					
WACN ID	System ID	RFSS ID	Unit ID Min	Unit ID Max	
00003 (3)	002 (2)	01	000000	06ffff	Edit Delete
00003 (3)	002 (2)	02	700000	700001	Edit Delete
00003 (3)	002 (2)	01	700002	FFFFFFF	Edit Delete
abcde (703710)	667 (1639)	09	000000	ffffff	Edit Delete

Figure 3-2 shows the group to home RFSS mapping table for this configuration.

Figure 3-2 Group Range to RFSS Home Mappings Table - Tri-site System

Group Range to RFSS Home Mappings							
WACN ID	System ID	RFSS ID	Group ID Min	Group ID Max			
00003 (3)	002 (2)	01	0000	7fff	Edit	Delete	
00003 (3)	002 (2)	01	8000	ffff	Edit	Delete	
abcde (703710)	667 (1639)	09	a000	ffff	Edit	Delete	

Configuring the System Watchdog

The system uses "monit" to ensure that essential applications are always running. This is a watchdog process that monitors a user-defined list of processes and restarts them in the event of failure. While this is not essential to enable the RNC to function, it provides a minimal level of redundancy in the event of failure.



Note

The "monit" process is installed as part of the installation.

To configure the system watchdog, perform the following procedure:

Procedure

- Step 1** Check that the "monit" application is installed. To do this, use the following command:
- ```
rpm -q monit
```
- Step 2** When "monit" is installed, modify /etc/monit.conf and ensure that the following lines are not commented out:

```
set daemon 10
set httpd port 2812 and
 allow localhost
 allow 192.168.1.0/255.255.255.0
 allow admin:monit
include /etc/monit.d/*
```

The above IP addresses are examples only.

**Step 3** Check that "monit" is configured to run at run levels 2 through 5. To do this, use the following command:

```
chkconfig --list | grep monit | grep -v mdmonitor
```

If the "monit" service is configured for the correct run levels, then the output from this command will be:

```
monit 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

If the "monit" service is not currently configured for the correct run levels, then the output from this command will be:

```
monit 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

If necessary, configure "monit" to run at the correct run levels. To do this, use the following command:

```
chkconfig monit on
```

**Step 4** Start "monit". To do this, use the following command:

```
/etc/init.d/monit start
```

This action will start the RNC.

**Step 5** Check that the RNC is running. To do this, use the following command:

```
monit summary | grep RncService
```

This will return an indication that the RncService is running, similar to:

```
Process 'RncService' running
```

**Step 6** Check that the web interface to "monit" is available. To do this, perform the following steps:

- a. Use a web browser to navigate to the IP address of the web interface. For example, 192.168.1.195:2812.

The above IP address is an example only.

- b. Type the username **admin** and password **monit** to log into the "Monit Service Manager".

The Monit Service Manager shows current information about the services being monitored, including system status, RncService process status and NifService process status.

Details (parameters/values) about each process can be viewed by clicking on a link that navigates to a dedicated page containing further information. The following actions are also available from these windows:

- System Status window; button for Disable/Enable Monitoring.
- RncService Process window; buttons for Start Service, Stop Service, Restart Service, Disable Monitoring.

## Configuring SNMP for Fault Management

To configure SNMP for fault management, perform the following procedure:

### Procedure

**Step 1** To configure snmpd for AgentX and SNMPv2 traps, add the following lines to /etc/snmp/snmpd.conf:

```
master agentx
trapcommunity public
trap2sink localhost
```

This allows AgentX and traps to be raised.

**Step 2** Change the permissions on the agentx socket for a non-root user as follows:

```
agentXSocket /tmp/agentx
agentXPerms 700 700 RncUser rfssadmin
```

This allows the RNC to communicate with the local snmpd process and then snmpd will raise traps to the localhost when required.

- Step 3** To configure snmptrapd to forward any SNMP traps to an external host, add the following lines to the file /etc/snmp/snmptrapd.conf:

```
authCommunity log,execute,net public
forward default <ip_address>
```

where <ip\_address> is the IP address to receive all the SNMP traps generated by this RNC. If this is the first installation of SNMP this file may not exist and will have to be created.

- Step 4** Start snmpd and snmptrap. To do this, use the following command:

```
service snmpd start
service snmptrapd start
```

## Configuring NTP

The Network Time Protocol (NTP) is used to synchronize the time between the nodes of a system. The time between the RNC and BSC must be synchronized, and the time between the RNC and other RNCs present on the system must also be synchronized. If the time is not synchronized, logging between nodes will not match, and call records will be incorrect.

The NTP daemon software is pre-installed on IPICS OS. The procedure described here details how to configure NTP at the RNC only.

The RNC typically acts as a master node for all the BSCs within its RFSS. Ideally the RNC would obtain a time reference from a public NTP time server, but where this is not allowable or possible, its own clock will suffice. While referencing time from the clock on the server does not assist with absolute time accuracy, it does force consistency between all the clocks on the system node.

To configure the NTP, perform the following procedure:

### Procedure

- Step 1** Check if "ntpd" is installed. To do this, use the following command:
- ```
service ntpd status
```
- Step 2** Configure the RNC as a client of a master server. To do this, perform the following steps:
- Open the file /etc/ntp.conf and ensure that there is a single server line as follows:

```
server <address>
```

where <address> is the IP name or IP number of the NTP server with which this RNC is synchronizing. If public internet access is available, ideally, 4-server address entries should be used to obtain optimum clock accuracy.
 - Where no public or local NTP servers are available, the RNC should be configured so that it is a clock reference.
 - Edit /etc/ntp.conf and ensure that the following exists as a duty server entry:

Server 127.127.1.0

Fudge 127.127.1.0 Stratum 10



Note Do not modify the IP address to match those in use for the RNC host. This address needs to be locally accessible, which should be on the local loopback address range. Further restrictions can be placed on IP ranges if required.

Step 3 Check that "ntpd" is configured to start at run levels 2 to 5. To do this, use the following command:

```
chkconfig --list | grep ntpd
```

If the "ntpd" service is configured for the correct run levels then the output from this command should be:

```
ntpd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Step 4 If necessary, configure the ntpd service to start at the correct run levels. To do this, use the following command:

```
chkconfig ntpd on
```

Step 5 Restart the ntp daemon. To do this, use the following command:

```
service ntpd restart
```

The clock may take a little while to initially synchronize with the server. To examine the ntpd status in more detail, view the file /var/log/messages for ntpd entries.

RNC Application

This section contains the following topics:

- [Starting and Stopping the RNC Using the Watchdog, page 3-15](#)
- [Manually Running the RNC, page 3-16](#)

Starting and Stopping the RNC Using the Watchdog

To start and stop the RNC from the command line the system watchdog "monit" should be used. You must run all of the following commands as the "root" user:

- To start the RNC, use the following command:

```
monit start RncService
```
- To stop the RNC, use the following command:

```
monit stop RncService
```
- To restart the RNC, use the following command:

```
monit restart RncService
```
- To determine whether the RNC is currently running, use the following command:

```
monit summary
```
- For a more detailed status report, use the following command:

monit status

- To view the system status in a web browser, see step 6 of the “Configuring the System Watchdog” section on page 3-12.

Manually Running the RNC

**Note**

While the RNC may be run manually for troubleshooting purposes, it should not be left in this state.

To run the RNC manually, perform the following procedure:

Procedure

- Step 1** Change directories to the RNC's configuration directory. To do this, use the following command:
- ```
cd /home/RncUser/config
```
- Step 2** Export the required library. To do this, use the following command:
- ```
export LD_LIBRARY_PATH=/home/RncUser/lib
```
- Step 3** Run the RNC process. To do this, use the following command:
- ```
../bin/Rnc
```

**Note**

To shut down the RNC when it has been started in this way, press <Ctrl>+<C>.

## SNMP Alarms and Alerts

Table 3-7 describes the SNMP alarms and alerts that can be raised by the RNC.

**Table 3-7** *SNMP Alarms and Alerts*

| Alarm/Alert Name             | Severity             | Source Identifier | Alarm or Alert |
|------------------------------|----------------------|-------------------|----------------|
| RNC Configuration Error      | Critical/Major/Minor | RNC               | Alert          |
| Failed Connecting To The NLR | Critical             | RNC               | Alarm          |



# CHAPTER 4

## Troubleshooting

---

This chapter contains a number of basic troubleshooting scenarios, including some of the most common problems that need to be resolved to get the RNC operating correctly following a new installation, configuration, or upgrade. This section does not cover all possible issues. General procedures for troubleshooting depend on the history of the RNC installation and the symptoms encountered.

This chapter includes the following sections:

- [The RNC Fails to Start, page 4-1](#)
- [The RNC Displays a “Could Not Create Sip Stack” Error, page 4-1](#)
- [The RNC Fails to Find Entries in "Rnc.config", page 4-2](#)
- [The RNC Cannot Communicate With the NLR, page 4-2](#)
- [The RNC Cannot Communicate With Entities Other Than the NLR, page 4-3](#)
- [The “monit” Command Reports a Duplicate, page 4-3](#)
- [The RPM Package Installation Hangs, page 4-4](#)
- [The SNMP Manager Does not Receive Alarms or Alerts, page 4-4](#)

### The RNC Fails to Start

#### Problem

The RNC fails to start, and the following error is displayed:

```
libstdc++.so.x not found
```

This condition is usually due to the version of Linux on which the RNC is installed, with either a newer or older version of the standard C++ shared library.

#### Solution

Install the required version of the standard C++ libraries. This can usually be found as a package prefixed with "libstdc++-compat".

### The RNC Displays a “Could Not Create Sip Stack” Error

#### Problem

The RNC starts, but the following error is displayed:

“Could Not Create Sip Stack ...”

This condition is usually caused by one of the following:

- The RNC could not find its configuration file.
- The IP address defined in the configuration file of the RNC is incorrect.
- Another RNC is already running.

#### Solution

Perform the following checks:

- Check that the RNC is not already running. To do this, use the following command:

```
monit status
```

- Check that the RNC configuration file exists and is named correctly. To do this, use the following command:

```
less /home/RncUser/config/Rnc.config
```

- Check that the RNC configuration file is owned by "RncUser" and has the correct permissions (750). To do this, use the following command:

```
ls -Lal /home/RncUser/config/Rnc.config
```

The correct output should be similar to:

```
-rwxr-x--- 1 RncUser rfssadmin 2734 Jan 2 01:02 Rnc.config
```

- Ensure that the IP address defined in the Rnc.config file in the parameter SIP.LocalIpAddress matches the IP address of the RNC.

## The RNC Fails to Find Entries in "Rnc.config"

#### Problem

The RNC starts, but it appears not to have found any entries in "Rnc.config".

This condition may be due to an invalid configuration file. In particular, where the file does not contain properly quoted entries, none of the configuration entries will be used and, where possible, the RNC will revert to using default values for all parameters. This will also cause the problem described in the [“The RNC Displays a “Could Not Create Sip Stack” Error”](#) section on page 4-1.

#### Solution

Ensure that every line entry has double quotes around both the configuration key and the value, for example:

```
"RG.RfssId"="1"
```

## The RNC Cannot Communicate With the NLR

#### Problem

The RNC starts, but there is no communication with the NLR.

This can be caused by either of the following conditions:

- Incorrect configuration of the NLR host name, database name, user or password in the Rnc.config file.
- MySQL is not running on the NLR host.

**Solution**

Perform the following checks:

- Check that the NLR parameters in the Rnc.config file are correct and match the setup for the NLR. These parameters are:

LrIfDatabaseName

LrIfDatabaseHost

LrIfDatabaseUser

LrIfDatabasePassword

- Check that MySQL is running. To do this, use the following command on the NLR host:

```
ps -fu mysql
```

The command should show the "mysql" process with some associated parameters. If this command does not display the "mysql" process, then MySQL must be started using the following command:

```
service mysqld start
```

## The RNC Cannot Communicate With Entities Other Than the NLR

**Problem**

The RNC starts, but there is no communication with entities other than the NLR. This condition is usually due to an incorrect /etc/hosts file configuration.

**Solution**

Check that the hosts file has an entry for each local site and each RFSS that the RNC needs to communicate with. Also check that these entries have the correct host names and IP addresses.

The format for the site and RFSS host names is very specific and must match that defined in the [“Configuring the System Host File”](#) section on page 3-2.

## The “monit” Command Reports a Duplicate

**Problem**

The "monit" command reports that there is a duplicate "/var/run/Rnc.pid".

This condition is usually due to duplicated RncService files in the directory /etc/monit.d. The /etc/monit.conf includes all extra files in the directory /etc/monit.d/

**Solution**

Ensure that there is only one RncService file present in the /etc/monit.d directory.

# The RPM Package Installation Hangs

## Problem

The RPM Package installation hangs. This can happen when the existing "Rnc" process is still running.

## Solution

Check that the existing "Rnc" process is not still running. If "monit" has not stopped "RncService", then "monit" will repeatedly attempt to start the "Rnc" process. This action will conflict with a new installation. The "Rnc" process should be stopped using "monit". If this action fails, a manual check of the "Rnc" process using the following command can show if the process is still running:

### **pgrep Rnc**

The remaining process can then be halted. To do this, use the following command:

### **pkill Rnc**

# The SNMP Manager Does not Receive Alarms or Alerts

## Problem

The SNMP Manager does not receive any alarms/alerts.

This can be caused by either of the following conditions:

- The RNC application is not connected with AgentX.
- The IP address configured in /etc/snmp/snmptrapd is incorrect.

## Solution

Perform the following checks:

- Check the snmpd configuration file to determine if "RncUser" has permission for the correct "snmp" agent. To do this, use the following command:

### **less /etc/snmp/snmpd.conf**

The correct configuration should be:

```
agentXSocket /tmp/agentx
agentXPerms 700 700 RncUser rfssadmin
```

- Check the snmptrapd configuration file to determine if the IP address is the IP address of the SNMP manager. To do this, use the following command:

### **less /etc/snmp/snmptrapd.conf**



## GLOSSARY

---

### A

- ABNF** Augmented Backus-Naur Form; used to describe syntax of fields in the ISSI standards.
- APCO** Association of Public-Safety Communications Officials. APCO Project 25 - digital conventional and trunked radio standard. Note that in this document, "APCO" as used invariably refers to APCO Project 25.

---

### B

- BS** Base Station.
- BSC** Base Station Controller.

---

### C

- COTS** Commercial Off The Shelf.

---

### D

- DVR** Digital Voice Recorder.

---

### H

- HLR** Home Location Register.
- Homed** A mobile unit that has its subscriber details defined in the NLR of a particular RFSS. This mobile unit may roam to other RFSSs, in which case it will be registered as a "visitor" unit once that RFSS confirms registration information with the home RFSS of the unit.

---

### I

- IP** Internet Protocol.
- ISSI** Inter-RF Sub System Interface; protocol used to communicate between RF Subsystems.

---

**L**

**Location** Indicates the identifier of the site at which the subscriber is currently registered.

---

**M**

**MR** Mobile Radio; used as an equivalent to Subscriber Unit (SU), terminal, portable or radio.

**MS** Mobile Station; used as an equivalent to SU, terminal, portable or radio.

---

**N**

**NIF** Network Interface Function.

**NLR** Network Location Register.

**NMS** Network Management System.

**NTP** Network Time Protocol.

---

**P**

**P25** See [APCO](#).

**P25CC** P25 Channel Controller.

**PCCT** P25CC Tool.

**PSTN** Public Switched Telephone Network.

**PTT** Push To Talk.

---

**R**

**RF** Radio Frequency.

**RPM** Red Hat Package Manager; this is both a software package file format, as well as a software package coded in that format. For the purposes of this guide, RPM is an extension package/executable used to install/uninstall software associated with the NLR.

**RFSS** Radio Frequency Subsystem.

**RNC** RFSS Network Controller.

**RSSI** Received Signal Strength Indicator.

---

|            |                               |
|------------|-------------------------------|
| <b>Rx</b>  | Receiver/Receive.             |
| <b>RTP</b> | Real-time Transport Protocol. |

---

|                   |                                                                                                                                               |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>S</b>          |                                                                                                                                               |
| <b>SG</b>         | Subscriber Group.                                                                                                                             |
| <b>SGID</b>       | Subscriber Group ID; 48 bit address used to uniquely identify an SG comprised of a 20 bit WACN ID, a 12 bit System ID, and a 16 bit Group ID. |
| <b>SIP</b>        | Session Initiation Protocol.                                                                                                                  |
| <b>SNMP</b>       | Simple Network Management Protocol.                                                                                                           |
| <b>SR</b>         | Soft Radio.                                                                                                                                   |
| <b>Status</b>     | Indicates the operating state of a subscriber or group.                                                                                       |
| <b>SU</b>         | Subscriber Unit; used as an equivalent term to mobile radio (MR), mobile station (MS), terminal, portable or radio.                           |
| <b>Subscriber</b> | A mobile unit that is a "member" of an RFSS and recognized as being homed at a particular RFSS.                                               |
| <b>SUID</b>       | Subscriber Unit ID; 56 bit address used to uniquely identify an SU comprised of a 20 bit WACN ID, a 12 bit System ID, and a 24 bit Unit ID.   |

---

|           |                       |
|-----------|-----------------------|
| <b>T</b>  |                       |
| <b>Tx</b> | Transmitter/Transmit. |

---

|                |                                                                                        |
|----------------|----------------------------------------------------------------------------------------|
| <b>U</b>       |                                                                                        |
| <b>Unit ID</b> | Mobile radio ID; 24 bit identifier used to represent a mobile radio unit (subscriber). |

---

|                |                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------|
| <b>V</b>       |                                                                                                      |
| <b>Visitor</b> | Indicates whether the subscriber or group is homed at its current RFSS or is a visitor to this RFSS. |
| <b>VLR</b>     | Visitor Location Register.                                                                           |

---

|             |                                   |
|-------------|-----------------------------------|
| <b>W</b>    |                                   |
| <b>WACN</b> | Wide Area Communications Network. |





## INDEX

---

### A

ABNF, defined [5-1](#)

APCO, defined [5-1](#)

---

### B

BS, defined [5-1](#)

BSC, defined [5-1](#)

---

### C

configuring

    gathering information [3-1](#)

    NLR for home RFSS information [3-10](#)

    NTP [3-14](#)

    SNMP for fault management [3-13](#)

    system host file [3-2](#)

    system watchdog [3-12](#)

COTS, defined [5-1](#)

---

### D

DVR, defined [5-1](#)

---

### H

hardware platform requirements [1-2](#)

HLR, defined [5-1](#)

homed, defined [5-1](#)

---

### I

interfaces

    RNC to NLR [2-1](#)

    RNC to other RFSS [2-2](#)

    RNC to sites in the local RFSS [2-1](#)

IP, defined [5-1](#)

ISSI, defined [5-1](#)

---

### L

location identifier, defined [5-2](#)

---

### M

manually running the RNC [3-16](#)

media controller parameters [3-8](#)

MR, defined [5-2](#)

MS, defined [5-2](#)

---

### N

network controller description [1-1](#)

NIF, defined [5-2](#)

NLR

    defined [5-2](#)

    parameters [3-7](#)

NMS, defined [5-2](#)

NTP, defined [5-2](#)

---

### P

P25, defined [5-2](#)

P25CC, defined [5-2](#)

PCCT, defined [5-2](#)

platform requirements

hardware [1-2](#)

software [1-3](#)

PSTN, defined [5-2](#)

PTT, defined [5-2](#)

---

## R

RF, defined [5-2](#)

RFSS, defined [5-2](#)

RNC

application [3-15](#)

defined [5-2](#)

global parameters [3-3](#)

installing [1-3](#)

interfaces, overview [2-1](#)

logging [2-2](#)

manually running [3-16](#)

starting and stopping using watchdog [3-15](#)

to NLR interface [2-1](#)

to other RFSS interfaces [2-2](#)

to sites in the local RFSS interfaces [2-1](#)

troubleshooting

cannot communicate with entities other than the NLR [4-3](#)

cannot communicate with the NLR [4-2](#)

displays a “could not create sip stack” error [4-1](#)

fails to find entries in rnc.config [4-2](#)

fails to start [4-1](#)

updating configuration file [3-3](#)

RPM

defined [5-2](#)

package installation hangs [4-4](#)

RSSI, defined [5-2](#)

RTP

defined [5-3](#)

stack parameters [3-10](#)

Rx, defined [5-3](#)

---

## S

SG, defined [5-3](#)

SGID, defined [5-3](#)

SIP

defined [5-3](#)

stack parameters [3-6](#)

SNMP

alarms and alerts [3-16](#)

defined [5-3](#)

manager does not receive alarms or alerts [4-4](#)

software, installing the RNC [1-3](#)

software platform requirements [1-3](#)

SR, defined [5-3](#)

stack parameters

RTP [3-10](#)

SIP [3-6](#)

starting and stopping RNC using watchdog [3-15](#)

status identifier, defined [5-3](#)

string definitions [3-10](#)

SU [5-3](#)

subscriber, defined [5-3](#)

SUID, defined [5-3](#)

---

## T

troubleshooting

monit command reports a duplicate [4-3](#)

RNC cannot communicate with entities other than the NLR [4-3](#)

RNC cannot communicate with the NLR [4-2](#)

RNC displays a “could not create sip stack” error [4-1](#)

RNC fails to find entries in rnc.config [4-2](#)

RNC fails to start [4-1](#)

SNMP manager does not receive alarms or alerts [4-4](#)

Tx, defined [5-3](#)

---

**U**

unit ID, defined [5-3](#)

updating the RNC configuration file [3-3](#)

user indications and RNC logging [2-2](#)

---

**V**

visitor, defined [5-3](#)

VLR, defined [5-3](#)

---

**W**

WACN, defined [5-3](#)

