



Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 9.0 R7
LTE RAN USER GUIDE

3HE 06506 AAAG TQZZA Edition 01

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Alcatel, Lucent, Alcatel-Lucent, the Alcatel-Lucent logo, and TiMetra are registered trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Copyright 2011-2012 Alcatel-Lucent.
All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

Alcatel-Lucent License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

- 1.1 Subject to the terms and conditions of this Agreement, Alcatel-Lucent grants to Customer and Customer accepts a nonexclusive, nontransferable license to use any software and related documentation provided by Alcatel-Lucent pursuant to this Agreement ("Licensed Program") for Customer's own internal use, solely in conjunction with hardware supplied or approved by Alcatel-Lucent. In case of equipment failure, Customer may use the Licensed Program on a backup system, but only for such limited time as is required to rectify the failure.
- 1.2 Customer acknowledges that Alcatel-Lucent may have encoded within the Licensed Program optional functionality and capacity (including, but not limited to, the number of equivalent nodes, delegate workstations, paths and partitions), which may be increased upon the purchase of the applicable license extensions.
- 1.3 Use of the Licensed Program may be subject to the issuance of an application key, which shall be conveyed to the Customer in the form of a Supplement to this End User License Agreement. The purchase of a license extension may require the issuance of a new application key.

2. PROTECTION AND SECURITY OF LICENSED PROGRAMS

- 2.1 Customer acknowledges and agrees that the Licensed Program contains proprietary and confidential information of Alcatel-Lucent and its third party suppliers, and agrees to keep such information confidential. Customer shall not disclose the Licensed Program except to its employees having a need to know, and only after they have been advised of its confidential and proprietary nature and have agreed to protect same.
- 2.2 All rights, title and interest in and to the Licensed Program, other than those expressly granted to Customer herein, shall remain vested in Alcatel-Lucent or its third party suppliers. Customer shall not, and shall prevent others from copying, translating, modifying, creating derivative works, reverse engineering, decompiling, encumbering or otherwise using the Licensed Program except as specifically authorized under this Agreement. Notwithstanding the foregoing, Customer is authorized to make one copy for its archival purposes only. All appropriate copyright and other proprietary notices and legends shall be placed on all Licensed Programs supplied by Alcatel-Lucent, and Customer shall maintain and reproduce such notices on any full or partial copies made by it.

3. TERM

- 3.1 This Agreement shall become effective for each Licensed Program upon delivery of the Licensed Program to Customer.

-
- 3.2 Alcatel-Lucent may terminate this Agreement: (a) upon notice to Customer if any amount payable to Alcatel-Lucent is not paid within thirty (30) days of the date on which payment is due; (b) if Customer becomes bankrupt, makes an assignment for the benefit of its creditors, or if its assets vest or become subject to the rights of any trustee, receiver or other administrator; (c) if bankruptcy, reorganization or insolvency proceedings are instituted against Customer and not dismissed within 15 days; or (d) if Customer breaches a material provision of this Agreement and such breach is not rectified within 15 days of receipt of notice of the breach from Alcatel-Lucent.
- 3.3 Upon termination of this Agreement, Customer shall return or destroy all copies of the Licensed Program. All obligations of Customer arising prior to termination, and those obligations relating to confidentiality and nonuse, shall survive termination.

4. CHARGES

- 4.1 Upon shipment of the Licensed Program, Alcatel-Lucent will invoice Customer for all fees, and any taxes, duties and other charges. Customer will be invoiced for any license extensions upon delivery of the new software application key or, if a new application key is not required, upon delivery of the extension. All amounts shall be due and payable within thirty (30) days of receipt of invoice, and interest will be charged on any overdue amounts at the rate of 1 1/2% per month (19.6% per annum).

5. SUPPORT AND UPGRADES

- 5.1 Customer shall receive software support and upgrades for the Licensed Program only to the extent provided for in the applicable Alcatel-Lucent software support policy in effect from time to time, and upon payment of any applicable fees. Unless expressly excluded, this Agreement shall be deemed to apply to all updates, upgrades, revisions, enhancements and other software which may be supplied by Alcatel-Lucent to Customer from time to time.

6. WARRANTIES AND INDEMNIFICATION

- 6.1 Alcatel-Lucent warrants that the Licensed Program as originally delivered to Customer will function substantially in accordance with the functional description set out in the associated user documentation for a period of 90 days from the date of shipment, when used in accordance with the user documentation. Alcatel-Lucent's sole liability and Customer's sole remedy for a breach of this warranty shall be Alcatel-Lucent's good faith efforts to rectify the nonconformity or, if after repeated efforts Alcatel-Lucent is unable to rectify the nonconformity, Alcatel-Lucent shall accept return of the Licensed Program and shall refund to Customer all amounts paid in respect thereof. This warranty is available only once in respect of each Licensed Program, and is not renewed by the payment of an extension charge or upgrade fee.

-
- 6.2 ALCATEL-LUCENT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, REPRESENTATIONS, COVENANTS OR CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OR REPRESENTATIONS OF WORKMANSHIP, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DURABILITY, OR THAT THE OPERATION OF THE LICENSED PROGRAM WILL BE ERROR FREE OR THAT THE LICENSED PROGRAMS WILL NOT INFRINGE UPON ANY THIRD PARTY RIGHTS.
- 6.3 Alcatel-Lucent shall defend and indemnify Customer in any action to the extent that it is based on a claim that the Licensed Program furnished by Alcatel-Lucent infringes any patent, copyright, trade secret or other intellectual property right, provided that Customer notifies Alcatel-Lucent within ten (10) days of the existence of the claim, gives Alcatel-Lucent sole control of the litigation or settlement of the claim, and provides all such assistance as Alcatel-Lucent may reasonably require. Notwithstanding the foregoing, Alcatel-Lucent shall have no liability if the claim results from any modification or unauthorized use of the Licensed Program by Customer, and Customer shall defend and indemnify Alcatel-Lucent against any such claim.
- 6.4 Alcatel-Lucent Products are intended for standard commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The Customer hereby agrees that the use, sale, license or other distribution of the Products for any such application without the prior written consent of Alcatel-Lucent, shall be at the Customer's sole risk. The Customer also agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the Products in such applications.

7. LIMITATION OF LIABILITY

- 7.1 IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ANY CLAIM, REGARDLESS OF VALUE OR NATURE, EXCEED THE AMOUNT PAID UNDER THIS AGREEMENT FOR THE LICENSED PROGRAM THAT IS THE SUBJECT MATTER OF THE CLAIM. IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ALL CLAIMS EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO ALCATEL-LUCENT HEREUNDER. NO PARTY SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER OR NOT SUCH DAMAGES ARE FORESEEABLE, AND/OR THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- 7.2 The foregoing provision limiting the liability of Alcatel-Lucent's employees, agents, officers and directors shall be deemed to be a trust provision, and shall be enforceable by such employees, agents, officers and directors as trust beneficiaries.

8. GENERAL

- 8.1 Under no circumstances shall either party be liable to the other for any failure to perform its obligations (other than the payment of any monies owing) where such failure results from causes beyond that party's reasonable control.
- 8.2 This Agreement constitutes the entire agreement between Alcatel-Lucent and Customer and supersedes all prior oral and written communications. All amendments shall be in writing and signed by authorized representatives of both parties.
- 8.3 If any provision of this Agreement is held to be invalid, illegal or unenforceable, it shall be severed and the remaining provisions shall continue in full force and effect.
- 8.4 The Licensed Program may contain freeware or shareware obtained by Alcatel-Lucent from a third party source. No license fee has been paid by Alcatel-Lucent for the inclusion of any such freeware or shareware, and no license fee is charged to Customer for its use. The Customer agrees to be bound by any license agreement for such freeware or shareware. CUSTOMER ACKNOWLEDGES AND AGREES THAT THE THIRD PARTY SOURCE PROVIDES NO WARRANTIES AND SHALL HAVE NO LIABILITY WHATSOEVER IN RESPECT OF CUSTOMER'S POSSESSION AND/OR USE OF THE FREWARE OR SHAREWARE.
- 8.5 Alcatel-Lucent shall have the right, at its own expense and upon reasonable written notice to Customer, to periodically inspect Customer's premises and such documents as it may reasonably require, for the exclusive purpose of verifying Customer's compliance with its obligations under this Agreement.
- 8.6 All notices shall be sent to the parties at the addresses listed above, or to any such address as may be specified from time to time. Notices shall be deemed to have been received five days after deposit with a post office when sent by registered or certified mail, postage prepaid and receipt requested.
- 8.7 If the Licensed Program is being acquired by or on behalf of any unit or agency of the United States Government, the following provision shall apply: If the Licensed Program is supplied to the Department of Defense, it shall be classified as "Commercial Computer Software" and the United States Government is acquiring only "restricted rights" in the Licensed Program as defined in DFARS 227-7202-1(a) and 227.7202-3(a), or equivalent. If the Licensed Program is supplied to any other unit or agency of the United States Government, rights will be defined in Clause 52.227-19 or 52.227-14 of the FAR, or if acquired by NASA, Clause 18-52.227-86(d) of the NASA Supplement to the FAR, or equivalent. If the software was acquired under a contract subject to the October 1988 Rights in Technical Data and Computer Software regulations, use, duplication and disclosure by the Government is subject to the restrictions set forth in DFARS 252-227.7013(c)(1)(ii) 1988, or equivalent.
- 8.8 Customer shall comply with all export regulations pertaining to the Licensed Program in effect from time to time. Without limiting the generality of the foregoing, Customer expressly warrants that it will not directly or indirectly export, reexport, or transship the Licensed Program in violation of any export laws, rules or regulations of Canada, the United States or the United Kingdom.

-
- 8.9 No term or provision of this Agreement shall be deemed waived and no breach excused unless such waiver or consent is in writing and signed by the party claimed to have waived or consented. The waiver by either party of any right hereunder, or of the failure to perform or of a breach by the other party, shall not be deemed to be a waiver of any other right hereunder or of any other breach or failure by such other party, whether of a similar nature or otherwise.
- 8.10 This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded.

Preface

The Preface provides general information about the 5620 Service Aware Manager documentation suite, including this guide.

Prerequisites

Readers of the 5620 SAM documentation suite are assumed to be familiar with the following:

- 5620 SAM software structure and components
- 5620 SAM GUI operations and tools
- typical 5620 SAM management tasks and procedures
- device and network management concepts

5620 SAM documentation suite

The 5620 SAM documentation suite describes the 5620 SAM and the associated network management of its supported devices. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

Table 1 lists the documents in the 5620 SAM customer documentation suite.

Table 1 5620 SAM customer documentation suite

Guide	Description
5620 SAM core documentation	
<i>5620 SAM Release Description</i>	The <i>5620 SAM Release Description</i> provides information about the new features associated with a 5620 SAM software release.

(1 of 4)

Guide	Description
<i>5620 SAM Planning Guide</i>	The <i>5620 SAM Planning Guide</i> provides information about 5620 SAM scalability and recommended hardware configurations.
<i>5620 SAM System Architecture Guide</i>	The <i>5620 SAM System Architecture Guide</i> is intended for technology officers and network planners to increase their knowledge of the 5620 SAM software structure and components. It describes the system structure, software components, and interfaces of the 5620 SAM. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.
<i>5620 SAM 5650 CPAM Installation and Upgrade Guide</i>	The <i>5620 SAM 5650 CPAM Installation and Upgrade Guide</i> provides OS considerations, configuration information, and procedures for the following: <ul style="list-style-type: none"> installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments 5620 SAM system migration to a different system conversion from a standalone to a redundant 5620 SAM system
<i>5620 SAM User Guide</i>	The <i>5620 SAM User Guide</i> provides information about using the 5620 SAM to manage the service-aware IP/MPLS network, including GUI basics, commissioning, service configuration, and policy management. The <i>5620 SAM User Guide</i> uses a task-based format. Each chapter contains: <ul style="list-style-type: none"> a workflow that describes the steps for configuring and using the functions detailed procedures that list the configurable parameters on the associated forms 5620 SAM management information specific to LTE network elements is covered in the <i>5620 SAM LTE ePC User Guide</i> and <i>5620 SAM LTE RAN User Guide</i> . 5620 SAM management information specific to 1830 PSS network elements is covered in the <i>5620 SAM Optical User Guide</i> .
<i>5620 SAM Integration Guide</i>	The <i>5620 SAM Integration Guide</i> provides procedures to allow the 5620 SAM to integrate with additional components.
<i>5620 SAM Supervision Module User Guide</i>	The <i>5620 SAM Supervision Module User Guide</i> provides information about how to configure and use the web-based 5620 SAM Supervision Module for fault management and at-a-glance network element monitoring.
<i>5620 SAM Scripts and Templates Developer Guide</i>	The <i>5620 SAM Scripts and Templates Developer Guide</i> provides information that allows you to develop, manage, and execute CLI-based or XML-based scripts or templates. The guide is intended for developers, skilled administrators, and operators who are expected to be familiar with the following: <ul style="list-style-type: none"> CLI scripting, XML, and the Velocity engine basic scripting or programming 5620 SAM functions
<i>5620 SAM Parameter Guide</i>	The <i>5620 SAM Parameter Guide</i> provides: <ul style="list-style-type: none"> parameter descriptions that include value ranges and default values parameter options and option descriptions parameter and option dependencies parameter mappings to the 5620 SAM-O XML equivalent property names There are dynamic links between the procedures in the <i>5620 SAM User Guide</i> and the parameter descriptions in the <i>5620 SAM Parameter Guide</i> . Parameters specific to LTE network elements are covered in the <i>5620 SAM LTE Parameter Reference</i> . Parameters specific to 1830 PSS network elements are covered in the <i>5620 SAM Optical Parameter Reference</i> .
<i>5620 SAM Statistics Management Guide</i>	The <i>5620 SAM Statistics Management Guide</i> provides information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM. Network examples are included.

(2 of 4)

Guide	Description
<i>5620 SAM Maintenance Guide</i>	The <i>5620 SAM Maintenance Guide</i> provides procedures for: <ul style="list-style-type: none"> generating baseline information for 5620 SAM applications performing daily, weekly, monthly, and as-required maintenance activities for 5620 SAM-managed networks
<i>5620 SAM Troubleshooting Guide</i>	The <i>5620 SAM Troubleshooting Guide</i> provides task-based procedures and user documentation to: <ul style="list-style-type: none"> help resolve issues in the managed and management networks identify the root cause and plan corrective action for: <ul style="list-style-type: none"> alarm conditions on a network object or customer service problems on customer services with no associated alarms list problem scenarios, possible solutions, and tools to help check: <ul style="list-style-type: none"> network management LANs network management platforms and operating systems 5620 SAM client GUIs and client OSS applications 5620 SAM servers 5620 SAM databases
<i>5620 SAM Alarm Reference</i>	The <i>5620 SAM Alarm Reference</i> provides a list of all alarms that the 5620 SAM can raise. The reference is organized by network element type.
<i>5620 SAM Glossary</i>	The <i>5620 SAM Glossary</i> defines terms and acronyms used in all of the 5620 SAM documentation, including 5620 SAM LTE documentation.
<i>5620 SAM Network Element Compatibility Guide</i>	The <i>5620 SAM Network Element Compatibility Guide</i> provides release-specific information about the compatibility of managed device features in 5620 SAM releases.
5620 SAM LTE documentation	
<i>5620 SAM LTE RAN Release Description</i>	The <i>5620 SAM LTE RAN Release Description</i> provides information about the LTE RAN features associated with the release.
<i>5620 SAM LTE ePC User Guide</i>	The <i>5620 SAM LTE ePC User Guide</i> describes how to discover, configure, and manage LTE ePC devices using the 5620 SAM. The guide is intended for LTE ePC network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire <i>5620 SAM LTE ePC User Guide</i> before you attempt to use the 5620 SAM in your LTE network.
<i>5620 SAM LTE RAN User Guide</i>	The <i>5620 SAM LTE RAN User Guide</i> describes how to discover, configure, and manage the Evolved NodeB, or eNodeB, using the 5620 SAM. The guide is intended for LTE RAN network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire <i>5620 SAM LTE RAN User Guide</i> before you attempt to use the 5620 SAM in your LTE network.
<i>5620 SAM LTE Parameter Reference</i>	The <i>5620 SAM LTE Parameter Reference</i> provides a list of all LTE ePC and LTE RAN parameters supported in the 5620 SAM.
5620 SAM-O documentation	
<i>5620 SAM XML OSS Interface Developer Guide</i>	The <i>5620 SAM XML OSS Interface Developer Guide</i> provides information that allows you to: <ul style="list-style-type: none"> use the 5620 SAM XML OSS interface to access network management information learn about the information model associated with the managed network develop OSS applications using the packaged methods, classes, data types, and objects necessary to manage 5620 SAM functions
<i>5620 SAM 3GPP OSS Interface Developer Guide</i>	The <i>5620 SAM 3GPP OSS Interface Developer Guide</i> describes the components and architecture of the 3GPP OSS interface to the 5620 SAM. It includes procedures and samples to assist OSS application developers to use the 3GPP interface to manage LTE devices.

(3 of 4)

Guide	Description
<i>5620 SAM 3GPP OSS Interface Compliance Statements</i>	The <i>5620 SAM 3GPP OSS Interface Compliance Statements</i> document describes the compliance of the 5620 SAM 3GPP OSS interface with the 3GPP standard.
5620 SAM optical documentation	
<i>5620 SAM Optical User Guide</i>	The <i>5620 SAM Optical User Guide</i> describes how to discover, configure, and manage optical devices using the 5620 SAM. The guide is intended for optical network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire <i>5620 SAM Optical User Guide</i> before you attempt to use the 5620 SAM in your network.
<i>5620 SAM Optical Parameter Reference</i>	The <i>5620 SAM Optical Parameter Reference</i> provides a list of all optical device parameters supported in the 5620 SAM.

(4 of 4)

Obtaining customer documentation

You can obtain 5620 SAM customer documentation:

- from the product
- on the web

On-product documentation

The 5620 SAM on-product customer documentation is delivered in HTML and PDF. Choose Help→User Documentation from the 5620 SAM client GUI to open the help system in a web browser.

The help system opens to the User Documentation Index, which provides a summary of and links to all 5620 SAM customer documents.

Click on the Using the help system tab on the User Documentation Index page to find usage tips for navigating and searching within the on-product customer documentation.

You can return to the User Documentation Index at any time by clicking on the Home icon, shown in Figure 1.

Figure 1 Home icon



Documentation on the web

The 5620 SAM customer documentation is available for download in PDF format from the Alcatel-Lucent Customer Support Center: <http://www.alcatel-lucent.com/myaccess>. If you are a new user and require access to this service, please contact your Alcatel-Lucent support representative.

In addition to the guides listed in Table 1, Release Notices and other documents not delivered on-product are posted to this site.

Working with PDFs

You can download PDFs of individual guides from the Alcatel-Lucent Customer Support Center, or you can choose to download a zip of all PDFs for a particular release.

You can use the Search function of Acrobat Reader (File→Search) to find a term in a PDF of any 5620 SAM document. To refine your search, use appropriate search options (for example, search for whole words only or enable case-sensitive searching). You can also search for a term in multiple PDFs at once, provided that they are located in the same directory. For more information, see the Help for Acrobat Reader.

Cross-book hotlinks, for example, from a parameter name in the *5620 SAM User Guide* to a description of that parameter in the *5620 SAM Parameter Guide*, work only if both PDF files are in the same directory.



Note — Users of Mozilla browsers may receive an error message when opening the PDF files in the 5620 SAM documentation suite. The offline storage and default cache values used by the browsers are the cause of the error message.

Alcatel-Lucent recommends changing the Mozilla Firefox offline storage or Mozilla 1.7 cache value to 100 Mbytes to eliminate the error message.

Documentation conventions

Table 2 lists the conventions that are used throughout the documentation.

Table 2 Documentation conventions

Convention	Description	Example
Key name	Press a keyboard key	Delete
Italics	Identifies a variable	<i>hostname</i>
Key+Key	Type the appropriate consecutive keystroke sequence	CTRL+G
Key-Key	Type the appropriate simultaneous keystroke sequence	CTRL-G
*	An asterisk is a wildcard character, which means “any character” in a search argument.	log_file*.txt
↵	Press the Return key	↵
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Alarm Policies

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are substeps in a procedure, they are identified by Roman numerals.

Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

- 1 This step offers two options. You must choose one of the following.
 - a This is one option.
 - b This is another option.
- 2 You must perform this step.

Example of substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

- 1 This step has a series of substeps that you must perform to complete the step. You must perform the following substeps.
 - i This is the first substep.
 - ii This is the second substep.
 - iii This is the third substep.
- 2 You must perform this step.

Measurement conventions

Measurements in this document are expressed in metric units and follow the *Système international d'unités* (SI) standard for abbreviation of metric units. If imperial measurements are included, they appear in brackets following the metric unit.

Table 3 lists the measurement symbols used in this document.

Table 3 Bits and bytes conventions

Measurement	Symbol
bit	b
byte	byte
kilobits per second	kb/s

Important information

The following conventions are used to indicate important information:



Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.



Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.



Note — Notes provide information that is, or may be, of special interest.

Contents

Preface	ix
Prerequisites.....	ix
5620 SAM documentation suite	ix
Obtaining customer documentation	xii
On-product documentation.....	xii
Documentation on the web.....	xii
Documentation conventions.....	xiii
Procedures with options or substeps.....	xiii
Measurement conventions	xiv
Important information.....	xv

Introduction

1 —	LTE RAN overview	1-1
1.1	LTE RAN overview	1-2
1.2	About this guide	1-2
	LTE customer documentation	1-3
1.3	Alcatel-Lucent LTE RAN product suite	1-3
	9952 WPS	1-3
	9400 NEM	1-3
	9959 NPO	1-3
	9958 WTA.....	1-3

2 —	LTE ePC and RAN management using the 5620 SAM	2-1
2.1	5620 SAM LTE NE management solution overview	2-2
	5620 SAM	2-3
	5620 SAM LTE RAN	2-3
	5620 SAM LTE ePC	2-4
	5620 SAM LTE 3GPP reference points	2-5
2.2	Supported 5620 SAM LTE NE management functions	2-5
2.3	Workflow for 5620 SAM LTE RAN management	2-6
3 —	5620 SAM LTE RAN features	3-1
3.1	5620 SAM Release 9.0.....	3-2

LTE RAN device discovery and configuration

4 —	LTE RAN configuration management	4-1
4.1	Configuration management overview	4-2
4.2	Self-configuration	4-2
4.3	Offline configuration	4-3
4.4	Online configuration	4-3
4.5	OSS support for eNodeB configuration management	4-3
	Interface structure.....	4-4
	Multiple-interface OSS design	4-5
5 —	eNodeB NE pre-provisioning and discovery	5-1
5.1	eNodeB pre-provisioning and discovery overview	5-2
	eNodeB pre-provisioning	5-2
	eNodeB discovery	5-2
	eNodeB rehomings and reconfiguration.....	5-3
5.2	Workflow to manage eNodeB pre-provisioning and discovery.....	5-3
5.3	eNodeB commissioning	5-4
5.4	eNodeB self-configuration	5-4
	Self-configuration policies	5-4
	Pre-provisioned NE instances.....	5-4
	The self-configuration process flow	5-5
	Self-configuration procedures.....	5-6
	Procedure 5-1 To create or modify an NE self-configuration policy.....	5-6
	Procedure 5-2 To create or modify a pre-provisioned NE instance.....	5-8
	Procedure 5-3 To delete a pre-provisioned NE instance	5-10
	Procedure 5-4 To delete the ENBEquipment object of a pre-provisioned NE instance	5-11
5.5	eNodeB discovery	5-11
	eNodeB discovery procedures	5-12
	Procedure 5-5 To configure the 5620 SAM to communicate with the eNodeB using SNMPv3.....	5-12

	Procedure 5-6 To create a discovery rule for eNodeB management by the 5620 SAM	5-14
	Procedure 5-7 To view and sort the deployment status of pre-provisioned NE instances.....	5-18
	Procedure 5-8 To run the self-configuration process flow for a pre-provisioned NE instance that has a status of Detected Node	5-19
	Procedure 5-9 To manage the discovery of an eNodeB.....	5-19
	Procedure 5-10 To ping an eNodeB.....	5-20
	Unidentified eNodeBs.....	5-21
	Procedure 5-11 To enter a value for an unset id parameter for an eNodeB.....	5-21
5.6	Unmanaging and deleting eNodeBs from the 5620 SAM network	5-22
	Procedure 5-12 To unmanage and delete an eNodeB.....	5-22
6 —	eNodeB offline configuration	6-1
6.1	Offline configuration overview.....	6-2
	Workorders	6-2
	Activation sessions and the activation manager.....	6-2
	Configuration snapshots.....	6-3
6.2	Workflow to manage offline configuration	6-3
6.3	Activation manager	6-4
	Running an activation session	6-5
	Activation manager procedures.....	6-6
	Procedure 6-1 To create an activation session	6-6
	Procedure 6-2 To deploy a WO using the activation manager.....	6-7
	Procedure 6-3 To delete an activation session	6-11
6.4	Configuration snapshots.....	6-11
	Configuration snapshot procedures	6-12
	Procedure 6-4 To create a snapshot instance.....	6-12
	Procedure 6-5 To take a configuration snapshot	6-15
	Procedure 6-6 To schedule a configuration snapshot.....	6-15
	Procedure 6-7 To delete a snapshot instance.....	6-18
6.5	WO and configuration snapshot file management	6-18
	File transfer between the 5620 SAM and the 9952 WPS.....	6-18
	Activation parameters in nms-server.xml	6-18
	WO import log management.....	6-19
	File management procedures	6-19
	Procedure 6-8 To configure WO and configuration snapshot file management on the 5620 SAM main server	6-20
	Procedure 6-9 To delete a WO from the 5620 SAM server	6-21
	Procedure 6-10 To view WO import logs.....	6-22
	Procedure 6-11 To delete a WO import log from the 5620 SAM server	6-22
	Procedure 6-12 To configure the default size constraint policy for WO import logs	6-22

7 —	eNodeB online configuration	7-1
7.1	Online configuration overview	7-2
	Object component tree	7-2
	Object logical view	7-3
	eNodeB parameters	7-3
7.2	Workflow to manage online configuration	7-5
7.3	ENB Equipment and eNodeB NE instance objects	7-5
	ENB Equipment and eNodeB NE instance property forms	7-6
	ENB Equipment and eNodeB NE instance procedures	7-6
	Procedure 7-1 To open an ENB Equipment properties form	7-7
	Procedure 7-2 To open an eNodeB NE instance properties form	7-8
	Procedure 7-3 To open the eNodeB NE instance logical view	7-9
	Procedure 7-4 To lock or unlock an eNodeB	7-9
7.4	Logical objects manager	7-10
	Logical objects manager procedures	7-10
	Procedure 7-5 To access and modify objects with the logical objects manager	7-11
7.5	9400 NEM support	7-11
	9400 NEM launch procedures	7-12
	Procedure 7-6 To launch the 9400 NEM from the 5620 SAM client GUI	7-12

LTE RAN management

8 —	LTE RAN device management	8-1
8.1	Overview	8-2
8.2	Workflow for LTE RAN management	8-2
8.3	eNodeB support	8-2
8.4	Inventory management	8-3
	Inventory procedures	8-3
	Procedure 8-1 To inventory eNodeB control board and base band cards	8-3
8.5	Object life cycle management	8-4
8.6	Bulk operations	8-4
8.7	eNodeB SSH sessions	8-5
8.8	IPv4 address migration	8-5
	Procedure 8-2 To migrate 5620 SAM management of eNodeBs between IPv4 addresses	8-5
8.9	IPv6 provisioning and migration	8-9
	IPv6 migration procedure	8-9
	Procedure 8-3 To migrate 5620 SAM management of eNodeBs from IPv4 to IPv6	8-10
8.10	Rehoming of eNodeBs between 5620 SAM servers	8-12
	Network configuration details	8-13
	Workflow for eNodeB rehoming	8-13
	Rehoming procedures	8-14
	Procedure 8-4 To prepare the main 5620 SAM source server	8-14

	Procedure 8-5 To prepare the main 5620 SAM target server	8-14
	Procedure 8-6 To prepare eNodeBs for rehomings	8-15
	Procedure 8-7 To discover and manage the rehomed eNodeBs on the target 5620 SAM server	8-17
	Procedure 8-8 To delete eNodeB objects on the source 5620 SAM server	8-18
	Procedure 8-9 To reverse the rehomings operation.....	8-19
9 —	LTE RAN licensing	9-1
9.1	RAN licensing overview.....	9-2
9.2	Workflow to manage RAN licensing	9-3
9.3	5620 SAM RAN license manager	9-3
	RAN license manager procedures	9-4
	Procedure 9-1 To import a RAN license file using the RAN license manager	9-5
	Procedure 9-2 To configure RAN license file reporting.....	9-5
	Procedure 9-3 To view the current RAN license file information.....	9-6
	Procedure 9-4 To generate a RAN license report.....	9-6
	Procedure 9-5 To recompute RAN license token consumption	9-7
9.4	RAN license consumption management.....	9-7
	Enumerated entitlements.....	9-7
	Feature entitlements	9-8
	Capacity entitlements	9-8
	Specific entitlements.....	9-8
	RAN license consumption management procedures	9-9
	Procedure 9-6 To configure license entitlement token consumption	9-9
10 —	LTE RAN EPS path management	10-1
10.1	EPS path topology map overview	10-2
	EPS path topology map window	10-2
	EPS path topology map panel	10-3
	Zoom in and out using a mouse	10-3
	EPS path topology map toolbar	10-4
	EPS path topology map management procedures	10-5
	Procedure 10-1 To open the EPS path topology map	10-6
	Procedure 10-2 To view EPS path topology map elements	10-6
	Procedure 10-3 To save a map view to a file	10-7
	Procedure 10-4 To zoom in and zoom out of a map	10-8
	Procedure 10-5 To view and modify EPS path information	10-9
10.2	EPS peers and paths	10-9
	EPS peers	10-10
	EPS paths	10-10
	Procedures	10-10
	Procedure 10-6 To view the properties of EPS peers from the EPS Peers and Paths form	10-11
	Procedure 10-7 To view the properties of EPS paths from the EPS Peers and Paths form	10-12
10.3	5620 SAM network topology maps	10-13

11 —	LTE RAN security	11-1
11.1	Overview	11-2
11.2	Workflow to configure LTE RAN security	11-2
11.3	5620 SAM user and group security	11-2
	Scope of command	11-2
11.4	RAN sharing	11-4
	RAN sharing - scope of command	11-4
	RAN sharing and the 5620 SAM Supervision Module	11-5
	RAN sharing procedures	11-5
	Procedure 11-1 To create an equipment group.....	11-6
	Procedure 11-2 To add NEs to an equipment group	11-7
	Procedure 11-3 To create a scope of command role	11-7
	Procedure 11-4 To create a scope of command profile	11-8
	Procedure 11-5 To create a span of control	11-9
	Procedure 11-6 To create a span of control profile.....	11-9
	Procedure 11-7 To create a 5620 SAM user group.....	11-11
	Procedure 11-8 To create a 5620 SAM user account	11-12
	Procedure 11-9 To copy a 5620 SAM user account	11-14
	Procedure 11-10 To search for inactive user accounts	11-14
	Procedure 11-11 To suspend or reinstate a 5620 SAM user account.....	11-15
11.5	eNodeB IPsec.....	11-15
	IPsec procedures	11-15
	Procedure 11-12 To enable or disable IPsec on an eNodeB.....	11-15
12 —	LTE RAN SON management	12-1
12.1	Overview	12-2
12.2	Workflow to configure SON functions.....	12-2
12.3	ANR.....	12-2
	IRAT ANR.....	12-3
	ANR procedures.....	12-3
	Procedure 12-1 To enable or disable the ANR function on an eNodeB.....	12-3
	Procedure 12-2 To enable or disable the IRAT ANR function on an eNodeB.....	12-4
	Procedure 12-3 To manually reset ANR and IRAT ANR on an eNodeB	12-5
	Procedure 12-4 To configure inter-LTE ANR parameters for neighbor relations	12-6
	Procedure 12-5 To configure IRAT ANR parameters for neighbor relations	12-7
12.4	PCI.....	12-7
	PCI procedures.....	12-7
	Procedure 12-6 To enable or disable PCI on an eNodeB.....	12-8
	Procedure 12-7 To configure PCI on an eNodeB	12-8

LTE RAN maintenance

13 –	LTE RAN device maintenance	13-1
13.1	Overview	13-2
13.2	Workflow to manage LTE RAN maintenance	13-2
13.3	NE maintenance preparation	13-2
	Network preparation	13-3
	Software upgrades	13-3
	Network preparation procedures	13-3
	Procedure 13-1 To assign a password to the samadmin user	13-4
13.4	eNodeB backup and restore	13-4
	Backup and restore procedures	13-5
	Procedure 13-2 To create or modify a RAN backup/restore policy.....	13-6
	Procedure 13-3 To delete a backup/restore policy.....	13-8
	Procedure 13-4 To configure the 5620 SAM to save RAN device configuration backups on a file system	13-8
	Procedure 13-5 To perform an immediate eNodeB backup or restore	13-9
	Procedure 13-6 To restore a device configuration backup other than the most recent	13-11
13.5	eNodeB software upgrades	13-11
	eNodeB software upgrade policies	13-12
	eNodeB software images	13-12
	eNodeB software upgrade procedures	13-13
	Procedure 13-7 To create an eNodeB software upgrade policy	13-13
	Procedure 13-8 To import an eNodeB software image into the 5620 SAM.....	13-15
	Procedure 13-9 To perform an immediate software upgrade on an eNodeB.....	13-16
	Procedure 13-10 To monitor software upgrade status.....	13-17
	Procedure 13-11 To delete an eNodeB software image from the 5620 SAM server	13-18
14 –	LTE RAN statistics	14-1
14.1	Overview	14-2
14.2	Workflow to manage LTE RAN statistics	14-2
14.3	eNodeB PM statistics.....	14-2
	Statistics collection overview	14-2
	RAN PM statistics procedures.....	14-4
	Procedure 14-1 To create or modify an eNodeB performance management policy	14-5
	Procedure 14-2 To set the PM maximum SNMP block size for an eNodeB.....	14-6
	Procedure 14-3 To configure PM statistics counter group selection for an eNodeB.....	14-7
14.4	LTE statistics configuration.....	14-7
	LTE PM statistics catch-up	14-8
	LTE PM statistics synchronization.....	14-8
	Statistics configuration procedures	14-8
	Procedure 14-4 To configure PM statistics catch-up on the 5620 SAM	14-8

14.5	PCMD	14-10
	PCMD procedures.....	14-10
	Procedure 14-5 To enable or disable PCMD on an eNodeB.....	14-11
14.6	eNodeB radio measurement	14-11
	Radio measurement procedures	14-13
	Procedure 14-6 To view eNodeB radio measurement using the 5620 SAM GUI	14-13
15	LTE RAN troubleshooting	15-1
15.1	Overview	15-2
15.2	Workflow to manage LTE RAN troubleshooting.....	15-2
15.3	Alarms and fault management	15-3
	Fault clearance procedures.....	15-3
	Procedure 15-1 To reset an eNodeB.....	15-3
	Procedure 15-2 To reset an eNodeB base band card or control board card.....	15-4
	Procedure 15-3 To reset an eNodeB RRH	15-4
	Procedure 15-4 To reset an eNodeB TRDU	15-5
	Procedure 15-5 To reset an eNodeB tower mounted amplifier	15-5
	Procedure 15-6 To reset an eNodeB remote electrical tilt	15-6
15.4	Event logging	15-7
	Event logging procedures	15-7
	Procedure 15-7 To view the events log for an eNodeB	15-7
	Procedure 15-8 To configure the event log policy for an eNodeB	15-7
	Procedure 15-9 To purge the statistics records	15-8
15.5	Device configuration and database troubleshooting.....	15-9
	Configuration misalignment	15-9
	Database fallback	15-9
	Database corruption	15-10
	Configuration and database troubleshooting procedures	15-10
	Procedure 15-10 To reconfigure an eNodeB database configuration.....	15-11
	Procedure 15-11 To resynchronize an eNodeB database configuration.....	15-12
15.6	Call trace	15-12
	Call trace scheduled tasks	15-14
	Alarms.....	15-14
	Statistics.....	15-14
	Security.....	15-14
	Data collection and storage	15-15
	Call trace management procedures	15-16
	Procedure 15-12 To configure global 5620 SAM call trace operation	15-16
	Procedure 15-13 To configure local eNodeB call trace operation	15-16
	Procedure 15-14 To create a call trace session using the global call trace management form	15-17
	Procedure 15-15 To create a call trace session using an eNodeB instance properties form.....	15-18
	Procedure 15-16 To activate a call trace session	15-19
	Procedure 15-17 To deactivate a call trace session	15-20
	Procedure 15-18 To delete a call trace session	15-20
	Procedure 15-19 To create a call trace scheduled task	15-21

Procedure 15-20 To control call trace scheduled task execution.....	15-22
Procedure 15-21 To manage the assignment of eNodeBs to call trace auxiliary-server pairs	15-23

Appendices

A.	eNodeB PM statistics counters	A-1
A.1	eNodeB PM statistics counters	A-2
A.2	eNodeB interface statistics	A-80
B.	RAN licenses	B-1
B.1	RAN license parameter mapping.....	B-2
B.2	LA2.0	B-2
B.3	TLA2.1	B-3
B.4	LA3.0	B-3
B.5	TLA3.0	B-4
B.6	LA 4.0	B-5
B.7	TLA4.0	B-6

Introduction

- 1 – LTE RAN overview
- 2 – LTE ePC and RAN management using the 5620 SAM
- 3 – 5620 SAM LTE RAN features

1 — *LTE RAN overview*

1.1 LTE RAN overview 1-2

1.2 About this guide 1-2

1.3 Alcatel-Lucent LTE RAN product suite 1-3

1.1 LTE RAN overview

The LTE RAN is the next generation of wireless broadband technology as outlined by the 3GPP and is the radio access component of the LTE solution. The eNodeB is the key NE of the LTE RAN and is the physical radio link between UE and the LTE ePC network. The eNodeB provides functions that include radio resource management, interfaces between eNodeBs and to ePC NEs, IP header compression, and bearer level control. The 5620 SAM is the OAM system that manages the eNodeB.

1.2 About this guide

The *5620 SAM LTE RAN User Guide* describes the various 5620 SAM GUI functions that are specific to eNodeB discovery, configuration, management, and maintenance. This guide also provides information about how the 5620 SAM interacts with other products in the Alcatel-Lucent LTE solution.

This guide does not provide descriptions or procedures for functions that apply only to non-LTE RAN devices, or descriptions of general 5620 SAM processes such as using the GUI or configuring the 5620 SAM client application. See the *5620 SAM User Guide* for more information about the general functions of the 5620 SAM and how to use the 5620 SAM to manage non-LTE NEs.

This guide contains the following volumes:

- Introduction—contains general LTE RAN information that includes the following:
 - an overview of the LTE RAN and the LTE product suite in the context of the 5620 SAM
 - an overview of the interaction between the LTE RAN and LTE ePC in the context of the 5620 SAM
 - new feature descriptions
- LTE RAN device configuration and discovery—contains information about discovering and configuring the eNodeB using the 5620 SAM, such as the following:
 - eNodeB self-configuration
 - device discovery
 - offline configuration
 - online configuration
- LTE RAN management—contains information about eNodeB support and NE management tasks that can be performed using the 5620 SAM, such as the following:
 - eNodeB support information
 - eNodeB inventory
 - IP migration (IPv4 to IPv4, and IPv4 to IPv6)
 - RAN feature and capacity licensing
 - EPS topology and path management
 - security configuration including user security and IPsec
 - SON management including ANR and PCI functions

- LTE RAN maintenance—contains information about eNodeB maintenance, statistics, and troubleshooting tasks that can be performed using the 5620 SAM, such as the following:
 - backup/restore
 - software upgrade
 - performance management statistics
 - troubleshooting including events logging, eNodeB database reconfiguration, and call trace
- Appendices—contains reference information, such as the following:
 - eNodeB PM counters
 - RAN license mapping to eNodeB parameters

LTE customer documentation

See the *Alcatel-Lucent 9400 | Customer Documentation Overview 418-000-010* for more information about the customer documentation in the Alcatel-Lucent LTE solution.

1.3 Alcatel-Lucent LTE RAN product suite

The Alcatel-Lucent LTE solution features several products that are designed to configure and optimize the RAN in conjunction with the 5620 SAM. The following products described in the following subsections interface with the 5620 SAM to facilitate RAN configuration and management.

9952 WPS

The 9952 WPS is the converged W-CDMA and LTE RAN tool for creating CM XML work order (WO) files that contain NE configuration data. The 9952 WPS can also convert configuration snapshot files into WOs. You can deploy WO files to the 5620 SAM managed network for NE configuration and pre-provisioning.

9400 NEM

The 9400 NEM provides OAM and LMT functions for the eNodeB such as parameter configuration, state management, and commissioning. You can launch the 9400 NEM from the 5620 SAM GUI.

9959 NPO

The 9959 NPO provides QoS information and cartographic tools for evaluating network performance and planning network expansion. You can use the 9959 NPO to optimize the LTE RAN by creating CM XML files in conjunction with the 9952 WPS. You must use the 5620 SAM to provide the 9959 NPO with updated network data by scheduling a daily configuration snapshot.

9958 WTA

The 9958 WTA is an analytic tool that is designed to perform post-processing on 3GPP-compliant call-trace data gathered by the 5620 SAM from the eNodeB and 9471 MME.

2 — *LTE ePC and RAN management using the 5620 SAM*

- 2.1 5620 SAM LTE NE management solution overview 2-2**
- 2.2 Supported 5620 SAM LTE NE management functions 2-5**
- 2.3 Workflow for 5620 SAM LTE RAN management 2-6**

2.1 5620 SAM LTE NE management solution overview

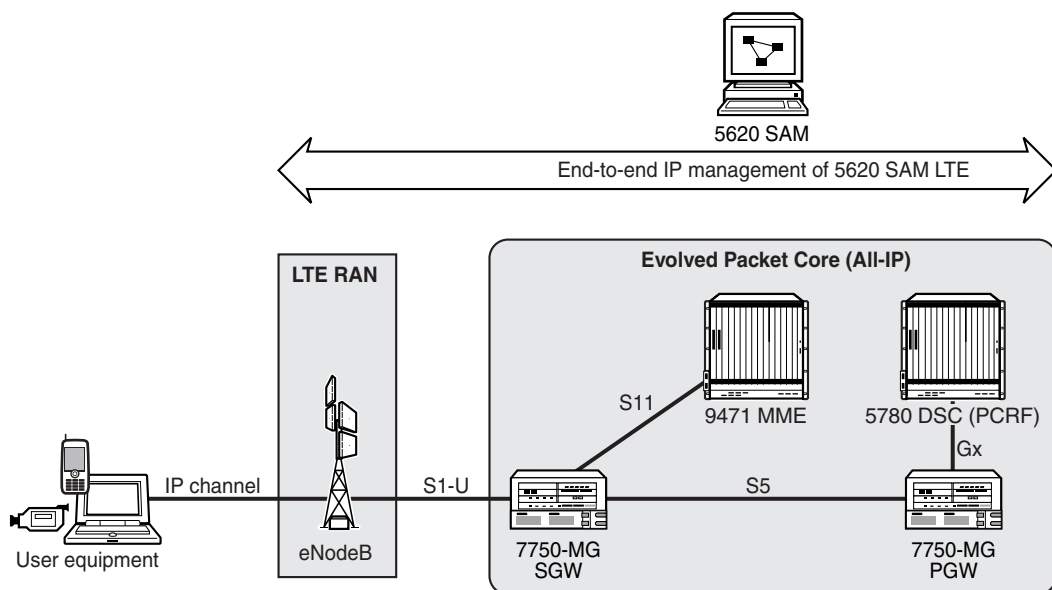
The 5620 SAM LTE NE management solution focuses on the equipment, configuration, fault, and state management of the ePC NEs, LTE interfaces, and mobile services that are used for mobile backhaul.

The 5620 SAM LTE NE management solution also supports the correlation of the LTE interfaces and mobile services with the underlying network transport layer to provide enhanced multi-layer monitoring and troubleshooting capabilities.

The 5620 SAM LTE NE management solution consists of the following components:

- 5620 SAM
- 5620 SAM LTE ePC
 - 7750 MG SGW
 - 7750 MG PGW
 - 9471 MME
 - 5780 DSC
- 5620 SAM LTE RAN (also referred to as the eUTRAN)
 - eNodeB

Figure 2-1 shows the 5620 SAM LTE NEs components and EPS interfaces that are managed in a typical LTE network.



20906

5620 SAM

The Alcatel-Lucent 5620 SAM enables integrated element, network and service-aware management of the products within the ePC and extends to RAN network devices, providing operators with end-to-end IP management within the eUTRAN, backhaul and core networks. The 5620 SAM manages both the mobile layer (bearers, QoS of traffic flows, GTP/PMIP tunnels) and the underlying transport layer attributes (bandwidth, pseudowires, LSPs) to provide cross-layer coordination and correlation.

The 5620 SAM also features enhanced advanced monitoring and service assurance capabilities to simplify the management of IP/MPLS-based networks. In particular, its automated troubleshooting functionality integrates physical, network routing and service topologies to simplify the process of fault isolation, minimizing service interruptions and reducing the possibility of human error.

Through a powerful, standards-based OSS interface, the 5620 SAM provides open, standards-based interfaces that easily adapt to existing OSS environments for faster and more cost-effective integration.

To further enhance their service assurance capabilities, mobile operators can deploy the 5620 SAM along with the Alcatel-Lucent 5650 Control Plane Assurance Manager, which enables operators to ensure network and service availability by detecting control-plane misconfigurations, malfunctions, and undetected routing updates. The 5650 CPAM offers real-time control plane visualization, proactive control plane surveillance, configuration validation and control plane diagnosis. In addition, by seamlessly integrating with the 5620 SAM, the Alcatel-Lucent 5650 CPAM gives carriers unprecedented manageability by unifying service, routing, MPLS and physical infrastructure management.

5620 SAM LTE RAN

5620 SAM LTE RAN support features the discovery, configuration, and management of the eNodeB. The 5620 SAM provides an end-to-end management solution of the all-IP LTE domain by managing RAN UE access points in addition to the ePC mobile backhaul.

eNodeB

The eNodeB is an enhanced BTS system for UE access to the LTE RAN network and LTE services in the 700 MHz spectrum. The core component of the eNodeB is the Alcatel-Lucent 9926 DBS, which is a converged product for W-CDMA, CDMA, and LTE in FDD and TDD. The 9926 DBS is referred to as the 9412 eNodeB when in compact form for LTE with integrated TRDUs, and when in distributed form with LTE-enabled remote radio heads (RRH). This guide generically refers to the 9926 DBS and 9412 eNodeB as the eNodeB.

The eNodeB provides the user plane and control plane protocol terminations for user equipment. The eNodeB uses the S1-MME interface to connect to the 9471 MME, the S1-U interface to connect to the 7750 MG SGW, and the X2 interface to connect to other eNodeBs.

5620 SAM LTE ePC

The 5620 SAM LTE ePC is an all-IP mobile core network for the LTE, and is a converged framework for packet-based real-time and non-real-time services. LTE is end-to-end all-IP: from mobile handsets and other terminal devices with embedded IP capabilities, over IP-based eNodeB, across the ePC and throughout the application domain. See the *5620 SAM LTE ePC User Guide* for more information about managing LTE ePC devices with the 5620 SAM.

The 5620 SAM LTE ePC consists of the following four components, each of which is defined by 3GPP standards.

7750 MG SGW

The 7750 MG SGW is a data plane element in the LTE network whose primary function is to manage user-plane mobility, and act as a demarcation point between the 5620 SAM RAN and the core network.

7750 MG PGW

The 7750 MG PGW is the termination point of the packet data interface towards the PDN. The 7750 MG PGW, which is the anchor point for sessions towards the external PDN, supports:

- policy enforcement, such as operator-defined rules for resource allocation and usage
- packet filtering, such as deep packet inspection for application type detection
- charging support, such as per-URL charging

9471 MME

The 9471 MME performs the signaling and control functions to manage the UE access to network connections, the assignment of network resources, and the management of the mobility states to support tracking, paging, roaming, and handovers. The 9471 MME controls all control-plane functions that are related to subscriber and session management. The 9471 MME supports the following functions:

- security procedures—end-user authentication as well as initiation and negotiation of ciphering and integrity protection algorithms
- terminal-to-network session handling—signaling procedures that are used to set up packet data context and negotiate associated parameters such as QoS
- idle terminal location management—tracking the area update process that is used to allow the network to join terminals for incoming sessions

5780 DSC

The Alcatel-Lucent 5780 DSC is a carrier-grade platform that provides the Policy and Charging Rules Function for 3G packet core and 4G evolved packet core networks according to the 3GPP Release 7 and 8 specifications.

The 5780 DSC allows service providers to manage and control network behavior based on their business rules, application requirements, network status, and subscriber entitlement and preferences. After these decisions are implemented, they are instantiated and enforced in the network as a set of network policies.

The 5780 DSC supports the following functions:

- provides the dynamic link between the data and user layer, and the application and subscriber layer
- authorizes the network connections and flow, and determines charging information
- determines and binds the required QoS policy
- determines the flow and charging rules during UE connections, including detection and policy control
- accepts AF requests for media components and charging
- notifies the AF about network events
- provides roaming support of the ePC solution
- allows operator control of subscription support, service assurance, and charging

5620 SAM LTE 3GPP reference points

LTE reference points, as shown in Figure 2-1, are based on the 3GPP standards and are created automatically when LTE peer devices are signaled. The following peers and reference points are supported in the 5620 SAM:

- 7750 MG SGW to eNodeB (S1-U)
- 7750 MG SGW to 7750 MG PGW (S5)
- 7750 MG SGW to 9471 MME (S11)
- 7750 MG PGW to 5780 DSC (Gx)
- 7750 MG PGW or 7750 MG SGW to CCF (Rf)
- 7750 MG SGW to OFCS (Ga)
- 7750 MG PGW to OFCS (Ga)
- eNodeB to 9471 MME (S1-MME)
- eNodeB to eNodeB (X2)

In addition, the 5620 SAM supports the following MME-specific reference points and EPS peers that have no interaction with other ePC components:

- Sm and M3 reference points for multimedia broadcast/multicast service
- SLs and SLg reference points for location-based services
- SBc reference point for warning message delivery
- X1_1 and X2 reference points for enhanced CALEA functionality

2.2 Supported 5620 SAM LTE NE management functions

The Alcatel-Lucent 5620 SAM, along with the 5650 CPAM, provides comprehensive element and end-to-end IP management for the Alcatel-Lucent LTE RAN and ePC NEs, LTE interfaces, and mobile services that are used for mobile backhaul.

Table 2-1 lists the 5620 SAM LTE NE management functions that are supported by the 5620 SAM.

Table 2-1 LTE NE management functions supported by the 5620 SAM

LTE NE management support	Discovery and mediation	Equipment	Configuration	Performance	State	Fault and alarm
5620 SAM LTE ePC (see the 5620 SAM LTE ePC User Guide)						
7750 MG SGW	✓	✓	✓	✓	✓	✓
7750 MG PGW	✓	✓	✓	✓	✓	✓
9471 MME	✓	✓	✓	✓	✓	✓
5780 DSC	✓	✓	—	—	✓	✓
5620 SAM LTE RAN						
eNodeB	✓	✓	✓	✓	✓	✓

2.3 Workflow for 5620 SAM LTE RAN management

The following workflow describes the sequence of high-level tasks required to manage LTE RAN using the 5620 SAM.

- 1 Pre-provision and discover eNodeBs using self-configuration; see chapter 5.
- 2 Configure eNodeBs using offline configuration; see chapter 6.
 - a Create WOs using the 9952 WPS.
 - b Deploy WOs to eNodeBs.
 - c Manage configuration snapshots.
- 3 Configure eNodeBs using online configuration; see chapter 7.
 - a Configure eNodeB objects using the 5620 SAM GUI or an OSS application.
 - b Configure eNodeB objects using a 5620 SAM GUI client to open the 9400 NEM.
- 4 Manage RAN feature and capacity licensing; see chapter 9.
- 5 Manage EPS paths and network topology; see chapter 10.
- 6 Manage LTE RAN security; see chapter 11.
- 7 Manage LTE RAN SON functions; see chapter 12.
 - a Configure the eNodeB ANR function.
 - b Configure the eNodeB PCI function.

- 8 Perform maintenance tasks; see chapter 13.
 - a Back up and restore RAN devices.
 - b Upgrade RAN device software, as required.
 - c Manage eNodeB component replacement tasks.
- 9 Manage LTE RAN statistics collection; see chapter 14.
 - a Configure the 5620 SAM to perform LTE RAN PM statistics collection.
 - b Configure eNodeB PM policies.
- 10 Troubleshoot RAN devices; see chapter 15.
 - a Monitor eNodeB events using the event logging function.
 - b Troubleshoot connection and path problems using the call trace function.
 - c Troubleshoot eNodeB NE database problems.
 - i Reconfigure eNodeBs to overwrite incorrect or corrupted device database configurations.
 - ii Resynchronize eNodeBs to reconcile the device configurations with the 5620 SAM database.
 - d Respond to alarms and perform remedial actions, as required.

3 — 5620 SAM LTE RAN features

3.1 5620 SAM Release 9.0 3-2

3.1 5620 SAM Release 9.0

Table 3-1 lists the features and functions added in the 5620 SAM Release 9.0 for LTE RAN support. See the *5620 SAM LTE ePC User Guide* for more information about features and functions for LTE ePC support. See the *5620 SAM User Guide* for more information about non-LTE features and functions.

Table 3-1 5620 SAM Release 9.0 LTE RAN features

Feature or function	Description	Reference for more information
5620 SAM Release 9.0 R7 features		
eNodeB reset	You can reset eNodeB components using reset buttons that are located the properties forms of the following objects: <ul style="list-style-type: none"> • tower mounted amplifiers (TMA) • remote electrical tilt (RET) 	See section 15.3 for more information.
IPv4 address migration	Added a section and procedure for performing IPv4 address migration.	See section 8.8 for more information.
5620 SAM Release 9.0 R6 LTE RAN features		
eNodeB reset	You can reset eNodeB components using reset buttons that are located the properties forms of the following objects: <ul style="list-style-type: none"> • ENB Equipment (causes a full device reset) • base band card • control board card • RRH • TRDU 	See section 15.3 for more information.
5620 SAM Release 9.0 R5 LTE RAN features		
eNodeB support	The 5620 SAM supports the discovery, configuration, and management of LA/TLA4.0 eNodeBs.	-
eNodeB rehomeing between 9471 MMEs	The 5620 SAM supports the configuration of RAN S1-MME and RAN SCTP profiles in order to facilitate eNodeB rehomeing between 9471 MMEs.	<i>5620 SAM LTE ePC User Guide</i>
LTE tracking areas	The 5620 SAM supports the configuration of global tracking areas and the assignment of LTE NEs to tracking areas.	<i>5620 SAM LTE ePC User Guide</i>
eNodeB licensing improvement	The 5620 SAM support for RAN license management is enhanced to include the following: <ul style="list-style-type: none"> • Specific license entitlements are supported. • Capacity license entitlements are replaced by specific entitlements. • You can manually recompute RAN license token consumption. 	See section 9.4 for more information about specific entitlements. See Procedure 9-5 for more information about manually recomputing RAN license consumption.
5620 SAM configuration evolution	The 5620 SAM support for CM XML configuration snapshots includes the following: <ul style="list-style-type: none"> • Configurable dynamic inclusion filters that allow you to include a specific subsets of eNodeBs. • Configuration snapshots can be compressed with Gzip. 	See section 6.4 for more information.

(1 of 2)

Feature or function	Description	Reference for more information
Performance management statistics	The 5620 SAM support for eNodeB performance management statistics includes the following: <ul style="list-style-type: none"> The viewing and historical plotting of eNodeB PM statistics in the 5620 SAM GUI is no longer supported. You can specify which eNodeB counter groups are reported to the 5620 SAM. 	See section 14.3 for more information about PM counter selection.
Wireless equipment management improvement	You can view a data feed of radio measurement parameters for eNodeBs.	See section 14.6 for more information about eNodeB radio measurement.
Support of LTE RAN sharing	Added a section and procedures for configuring RAN sharing in the 5620 SAM network.	See section 11.4 for more information.
Support of IRAT ANR	The 5620 SAM support for eNodeB SON functions is enhanced to include IRAT ANR.	See section 12.3 for more information.
ICMP ping	The 5620 SAM supports ICMP ping of eNodeBs.	See Procedure 5-10 for more information.
Discontinued support for 5620 SAM Release 9.0 R5		
IPsec and ANR profiles	The configuration and deployment of IPsec and ANR profiles is no longer supported. You can use offline and online configuration to configure ANR and IPsec parameters for eNodeBs.	-
5620 SAM Release 9.0 R4 features		
No LTE RAN management features have been added for 5620 SAM Release 9.0 R4.		
5620 SAM Release 9.0 R3 features		
No LTE RAN management features have been added for 5620 SAM Release 9.0 R3.		
5620 SAM Release 9.0 R2 features		
No LTE RAN management features have been added for 5620 SAM Release 9.0 R2.		
5620 SAM Release 9.0 R1 features		
No LTE RAN management features have been added for 5620 SAM Release 9.0 R1.		

(2 of 2)

LTE RAN device discovery and configuration

- 4 – LTE RAN configuration management
- 5 – eNodeB NE pre-provisioning and discovery
- 6 – eNodeB offline configuration
- 7 – eNodeB online configuration

4 — *LTE RAN configuration management*

- 4.1 Configuration management overview 4-2
- 4.2 Self-configuration 4-2
- 4.3 Offline configuration 4-3
- 4.4 Online configuration 4-3
- 4.5 OSS support for eNodeB configuration management 4-3

4.1 Configuration management overview

Configuration management is defined as operator-driven configuration of the eNodeB. The 5620 SAM provides operators with the following methods for performing configuration management on the eNodeB:

- self-configuration
- offline configuration
- online configuration

4.2 Self-configuration

Self-configuration is a key feature of the 3GPP SON specification for RAN device self-organization. Self-configuration streamlines and automates the process of adding large numbers of eNodeBs to the 5620 SAM network. Self-configuration of RAN devices with the 5620 SAM requires the completion of the following steps:

- 1 The creation of one or more WOs for device configuration, based on a pre-planned vision of the deployed RAN.
- 2 The automatic or manual creation of pre-provisioned NE instances that contain the configuration data of the WOs described in the previous step.
- 3 The creation of a mediation security policy that specifies the transport protocols that are used to communicate with the devices.
- 4 The creation of one or more self-configuration policies that specify the steps followed by the self-configuration process flow during device discovery.
- 5 The creation of a discovery rule that incorporates the mediation security and self-configuration policies, in addition to rule elements that specify eNodeB IP addresses or subnets.
- 6 The activation of the discovery rule in order to trigger active scanning of specified IP ranges.
- 7 The automatic association between pre-provisioned NE instances and newly discovered devices in order to activate of the self-configuration process flow for the appropriate devices.
- 8 The execution of the self-configuration process flow, which may include device software upgrade/downgrade, configuration deployment, and administrative enabling of the device.
- 9 The successful resynchronization of eNodeBs with the 5620 SAM.

WO creation is ideally performed well in advance of eNodeB commissioning using the 9952 WPS. The 5620 SAM can activate a WO containing hundreds of RAN devices and use the contained configuration data to automatically create an equivalent number of pre-provisioned NE instances.

See section [5.4](#) for more information about self-configuration.

4.3 Offline configuration

Offline configuration is the process of using an application that is external to the 5620 SAM in order to create network configuration templates that can be deployed to the 5620 SAM network.

Operators can use the 9952 WPS to create CM XML WO files, import the WO files into the 5620 SAM, and use the 5620 SAM activation manager to deploy the WO files to eNodeBs. Conversely, operators can use the 5620 SAM to generate CM XML configuration snapshot files, import the files into the 9952 WPS, and convert the configuration snapshots into WOs. Configuration snapshots can also be used to provide the 9959 NPO with updated network data.

You can set up a connection for transferring CM XML files between the 5620 SAM and the 9952 WPS by specifying the 5620 SAM as a live server repository in the 9952 WPS. File transfer via FTP is also supported. See the *9952 WPS User Guide* for more information.



Note — You must enable SSL on the 5620 SAM main server before you can use the live server repository function of the 9952 WPS to import and export CM XML files.

See chapter 6 for more information about offline configuration.

4.4 Online configuration

Online configuration is the process of using the 5620 SAM GUI to configure eNodeB parameters individually, or in groups using the logical objects manager. Online configuration also includes the use of OSS interfaces to configure the eNodeB, and eNodeB NE configuration using the 9400 NEM.

See chapter 7 for more information about online configuration.

4.5 OSS support for eNodeB configuration management

The 5620 SAM provides OSS support for eNodeB configuration management via the 5620 SAM-O, the 3GPP-compliant 5620 SAM-O CORBA interface, and through dedicated files on the 5620 SAM server file system. See the following documents for more information:

- *5620 SAM XML OSS Interface Developer Guide*
- *5620 SAM 3GPP OSS Interface Developer Guide*
- *5620 SAM 3GPP OSS Interface Compliance Statements*

Table 4-1 describes the interfaces and supported functions for eNodeB configuration management over OSS.

Table 4-1 CM interfaces and supported functions

Interface	CM inventory	CM provisioning	Fault management	Performance management
5620 SAM-O	✓	✓	✓	✓
5620 SAM-O CORBA	✓		✓	
PM statistics file				✓
CM configuration snapshot file	✓	✓		

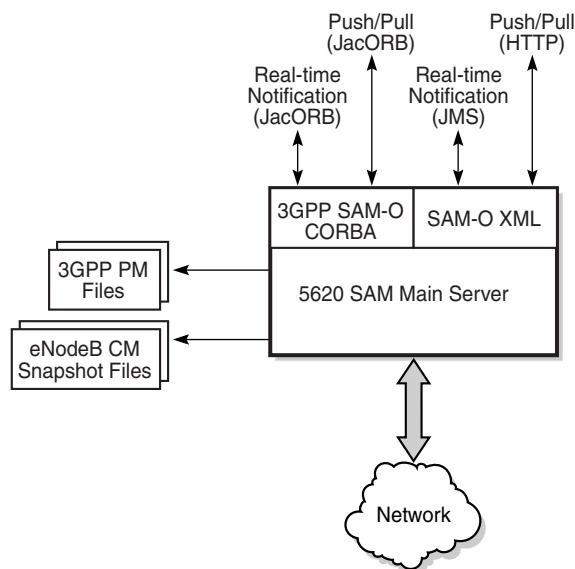
Interface structure

The 5620 SAM uses the following interfaces to communicate with OSS applications for LTE RAN management:

- 5620 SAM-O XML
 - Real-time notification (JMS)
 - Push/pull (HTTP)
- 3GPP 5620 SAM-O CORBA
 - Real-time notification (JacORB)
 - Push/pull (JacORB)
- 3GPP performance management files
- eNodeB configuration snapshot files

See Figure 4-1 for more information about the OSSI structure for LTE RAN management.

Figure 4-1 LTE RAN OSS interface structure



21851

Multiple-interface OSS design

Developing an OSS application that interacts with multiple interfaces may require additional effort and complicate the OSS design. Alcatel-Lucent strongly recommends that OSS architects carefully consider whether the OSS should interact with more than one interface.

5 — *eNodeB NE pre-provisioning and discovery*

- 5.1 eNodeB pre-provisioning and discovery overview 5-2
- 5.2 Workflow to manage eNodeB pre-provisioning and discovery 5-3
- 5.3 eNodeB commissioning 5-4
- 5.4 eNodeB self-configuration 5-4
- 5.5 eNodeB discovery 5-11
- 5.6 Unmanaging and deleting eNodeBs from the 5620 SAM network 5-22

5.1 eNodeB pre-provisioning and discovery overview

This chapter describes eNodeB pre-provisioning, discovery, and hardware configuration tasks.

eNodeB pre-provisioning

Pre-provisioning of the LTE RAN facilitates 5620 SAM management and configuration of a large number of NEs. Pre-provisioned eNodeB instances are configuration templates that the 5620 SAM can match with a real eNodeB using a discovery rule and associated self-configuration policy. You can create pre-provisioned eNodeBs by configuring a pre-provisioned NE instance, or by deploying a CM XML WO using the 5620 SAM activation manager. Pre-provisioning of eNodeBs is also called self-configuration. See section 5.4 for more information.

eNodeB discovery

The 5620 SAM uses SNMP to discover NEs by scanning the network according to the specified IP addresses or IP ranges. Discovery rules contain the rule elements that specify which IP addresses or ranges are included or excluded in the discovery process. When the 5620 SAM discovers an NE, it sets the NE status to Managed and adds the device properties to the 5620 SAM database.

See the *5620 SAM User Guide* for more information about NE discovery and management.

eNodeB site ID

The 5620 SAM uses a string value, instead of a management or system IP address, to represent an eNodeB in the network. This string identifier is the value of the *id* parameter of the ENBEquipment object. The ENBEquipment object is the root of the NetConf tree that contains the parameters and properties of the eNodeB MIM.

The 5620 SAM classifies eNodeBs without a value entered for the ENBEquipment id object as unidentified nodes and stops the discovery process. Perform Procedure 5-11 to enter an identifying value for unidentified nodes and allow the discovery to proceed.



Note 1 — The value of the id property of the ENBEquipment object must be unique because the 5620 SAM uses this value to identify the eNodeB in the network.

Note 2 — You must unmanage and remanage an eNodeB if you change the ENBEquipment id value after device discovery by the 5620 SAM.

Note 3 — The id property is the 5620 SAM equivalent of the uniqueName parameter in the eNodeB MIM. It is used to identify objects for operator use and for PM reporting. It must be set by the 9400 NEM.

eNodeB rehomming and reconfiguration

See *Alcatel-Lucent 9412 eNodeB | Release LAx.x-TLx.x eNodeB Reconfiguration Procedures 418-000-311* for information about the following tasks:

- rehomming of eNodeBs between 5620 SAM servers (see also section 8.10 of this document)
- adding a new eCEM to an eNodeB
- removing an eCEM from an eNodeB
- adding a new cell to an eNodeB
- connecting an eNodeB to a 9471 MME pool
- reparenting an eNodeB from one 9471 MME to another 9471 MME

5.2 Workflow to manage eNodeB pre-provisioning and discovery

The following workflow describes the sequence of high-level tasks required to pre-provision, configure, and discover eNodeBs for 5620 SAM management.

- 1 Create self-configuration policies that specify the level of operator involvement in the configuration process during eNodeB discovery. See Procedure 5-1.
- 2 Create pre-provisioned NE instances to serve as placeholders for undiscovered eNodeBs, as required. See Procedure 5-2.
- 3 Manage CM XML deployment to automatically create pre-provisioned NE instances by deploying WOs, as required.
 - i Create an activation session. See Procedure 6-1.
 - ii Deploy the WO to the 5620 SAM network. See Procedure 6-2.
- 4 Create an SNMPv3 user for eNodeB management, and create one or more mediation security policies for eNodeB management. See Procedure 5-5 for more information.
- 5 Create a discovery rule for self-configuration. See Procedure 5-6. The discovery rule must contain the following:
 - self-configuration policy
 - pre-provisioned NE instance
 - eNodeB-specific mediation security policy
 - rule elements that contain eNodeB IP addresses or IP address ranges
- 6 View and sort the deployment status of pre-provisioned NE instances. Procedure 5-7.
- 7 Run the self-configuration process flow for discovered eNodeBs. See Procedure 5-8.
- 8 Scan the network according to the discovery rules and manage NE discovery. See Procedure 5-9 for more information.

- 9 Ping eNodeBs, as required. See Procedure [5-10](#).
- 10 Unmanage and delete eNodeBs from the 5620 SAM managed network, as required. See Procedure [5-12](#).

5.3 eNodeB commissioning

Commissioning of the eNodeB requires the configuration of alpha and beta parameters in the SNMP MIB using the 9400 NEM. Commissioning is generally performed by on-site technicians with an LMT. Parameters that are not configured are set to their factory defaults.



Note — A static route must be configured if the eNodeB is in a different subnet than the 5620 SAM.

5.4 eNodeB self-configuration

Alcatel-Lucent recommends self-configuration as the method for discovering and configuring eNodeBs for management by the 5620 SAM. Procedures [5-1](#) and [5-2](#) describe the steps required to manually create self-configuration policies and pre-provisioned NE instances. See chapter [6](#) for more information about automatically creating pre-provisioned NE instances by activating a WO.

Self-configuration policies

Self-configuration policies determine the stages of the process flow followed by the 5620 SAM for eNodeBs that are identified as candidates for self-configuration. You can configure the 5620 SAM to perform, skip, or pause for operator intervention at one or more stages. The self-configuration process flow includes the stages listed below.

- The application of software upgrades as specified in the NE self-configuration policy and associated RAN software upgrade policy.
- The deployment of the configuration data contained by the pre-provisioned NE instance with an automatically created activation session.
- Setting the administrative state of successfully configured eNodeBs to Up.

Perform Procedure [5-1](#) to create or modify a self-configuration policy. Perform Procedure [5-8](#) to manually run the self-configuration process flow.

Pre-provisioned NE instances

Pre-provisioned NE instances are placeholder NE templates that contain the configuration data that is deployed to an eNodeB upon discovery. When you use the activation manager to activate an NE WO that creates an ENBEquipment object with an identifier that does not match any existing pre-provisioned or discovered eNodeBs, the 5620 SAM automatically creates a corresponding pre-provisioned NE instance. This function helps to facilitate LTE RAN pre-provisioning.

Pre-provisioned NE instances can be associated with a software upgrade policy that functions as an override to the default software upgrade policy.

Perform Procedure 5-2 to manually create or modify a pre-provisioned NE instance.



Note — Configuration deployment overwrites the existing NetConf tree on the eNodeB. Prior device configuration will be lost.

The self-configuration process flow

The self-configuration process flow is a series of configurable actions, specified in a self-configuration policy, that are taken by the 5620 SAM when an eNodeB that matches a pre-provisioned NE instance is discovered. When the 5620 SAM discovery control matches a newly discovered eNodeB with a pre-provisioned NE instance, the state of the pre-provisioned NE instance changes from Awaiting Node to Detected Node.

When the pre-provisioned NE instance is configured for Auto Start, the process flow starts automatically. Checkpoints specify points in the process flow that will pause and await operator intervention. When no checkpoints are selected, the process flow runs to completion without operator intervention. The steps that are required to run the self-configuration process flow are described in Procedure 5-8.



Note 1 — An eNodeB that is under a configuration lock due to a started activation session cannot be configured via online configuration.

Note 2 — eNodeBs that are manually set to an Administrative State of Locked can only be configured or modified after the state of the eNodeB is set to Unlocked by a 5620 SAM operator.

During the SW Upgrade stage of the process flow, the 5620 SAM verifies whether the software version specified in the pre-provisioned NE instance and self-configuration policy match the software version of the newly discovered eNodeB. If the software version of the eNodeB is lower than the specified version, then the 5620 SAM automatically reconfigures the SFTP target of the eNodeB and initiates a software update. If the software version in the eNodeB is higher than the software version specified by the pre-provisioned NE instance and self-configuration policy, the 5620 SAM raises a software version mismatch alarm.

During the Configuration Deployment stage of the process flow, the 5620 SAM deploys the parameter configuration specified in the pre-provisioned NE instance that corresponds to the newly discovered eNodeB.

The Administrative Enable stage of the process flow is when the 5620 SAM sets the administrative state of the newly discovered eNodeB to Up and performs a full resynchronization of the device. The 5620 SAM changes the eNodeB state to Managed and raises an informational alarm to notify operators of a successful self-configuration event.

Self-configuration procedures

Perform the following procedures to configure the policies and objects required for eNodeB self-configuration in the 5620 SAM network. See the *5620 SAM Parameter Guide* for descriptions of the parameters in the following procedures.

Procedure 5-1 To create or modify an NE self-configuration policy

Self-configuration of the eNodeB by the 5620 SAM requires the creation of both an NE self-configuration policy and a pre-provisioned NE instance.

- 1 Choose Administration→NE Self Config Policy Manager from the 5620 SAM main menu. The NE Self Config Policy Manager form opens.
- 2 Perform one of the following:
 - a Create an NE self-configuration policy by clicking on the Create button. The NE Self Config Policy (Create) form opens. Go to step 3.
 - b Modify an NE self-configuration policy:
 - i Configure the filter criteria, if required, and click on the Search button. A list of self-configuration policies is displayed.
 - ii Choose an NE self-configuration policy from the list and click on the Properties button. The NE Self Config Policy (Edit) form opens. Go to step 3.
- 3 Configure the Name parameter.
- 4 Click on the Select button for the Node Type and choose a device from the list.
- 5 Configure the following parameters in the Process Flow panel:
 - Auto Start
 - SW Upgrade—enabling this parameter will display the Software Upgrade panel.
 - Configuration Deployment
 - Administrative Enable




Note — The “Process Flow” parameters specify the actions that are performed by the 5620 SAM during NE self-configuration.

- 6 Configure the parameters in the Checkpoints Before panel:
 - SW Upgrade
 - Configuration Deployment
 - Administrative Enable



Note — The “Checkpoints Before” parameters specify the actions that require operator intervention before being performed by the 5620 SAM.

- 7 Perform one of the following:
 - a If the SW Upgrade check box is selected and the Software Upgrade panel is displayed, go to step 8.
 - b If the SW Upgrade check box is not selected and the Software Upgrade panel is not displayed, go to step 10.
 - 8 Perform one of the following:
 - a Choose a RAN node software upgrade policy:
 - i Click on the Select button for the Policy ID in the Software Upgrade panel. The Select RAN Node Software Upgrade Policy form opens.
 - ii Configure the filter criteria, if required, and click on the Search button. A list of RAN node software upgrade policies is displayed.
 - iii Choose a RAN node software upgrade policy from the list and click on the OK button to return to the NE Self Config Policy form. Go to step 9.
 - b Create a RAN node software upgrade policy:
 - i Click on the Select button for the Policy ID in the Software Upgrade panel. The Select RAN Node Software Upgrade Policy form opens.
 - ii Perform Procedure 13-7.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of RAN node software upgrade policies is displayed.
 - iv Choose a RAN node software upgrade policy from the list and click on the OK button to return to the NE Self Config Policy form. Go to step 9.
 - 9 Choose a software image:
 - i Click on the Select button for the Software Release in the Software Upgrade panel. The Select Software Image form opens.
-  **Note** — You must import a software image by performing Procedure 13-8 before you can choose a software image.
- ii Choose a software image from the list and click on the OK button to return to the NE Self Config Policy form.
 - 10 Click on the OK button to close the form and save the NE self-configuration policy. When you modify an existing NE self-configuration policy, a dialog box appears. Click on the Yes button to close the dialog box.
 - 11 Close the NE Self Config Policy Manager form.
-

Procedure 5-2 To create or modify a pre-provisioned NE instance

This procedure describes how to manually configure a pre-provisioned NE instance using the 5620 SAM GUI. Perform Procedure 6-1 and 6-2 to automatically create a pre-provisioned NE instance by deploying a WO.

- 1 Choose Administration→Pre-Provisioned NE Manager from the 5620 SAM main menu. The Pre-Provisioned NE Manager form opens.
- 2 Perform one of the following:
 - a To create a pre-provisioned NE instance, click on the Create button. The Pre-Provisioned NE (Create) form opens with the General tab displayed. Go to step 3.
 - b To modify an existing pre-provisioned NE instance:
 - i Configure the filter criteria, if required, and click on the Search button. A list of pre-provisioned NE instances is displayed.
 - ii Choose a pre-provisioned NE instance from the list and click on the Properties button. The Pre-Provisioned NE (Edit) form opens with the General tab displayed. Go to step 7.
- 3 Configure the Network Element ID parameter.



Note — The Network Element ID parameter is used as the identifier for an eNodeB in the network. The Network Element ID of a pre-provisioned NE instance must match the ENBEquipment *id* value of the corresponding eNodeB for the two to be matched in the network upon discovery by the 5620 SAM.

- 4 Click on the Select button for the Network Element Type and choose an eNodeB type from the list.
- 5 Click on the Select button for the Network Element Version and choose a version from the list.
- 6 Configure the Chassis Type parameter.
- 7 Click on the Options tab button.
- 8 Configure the parameters:
 - Active Management IP
 - Hardware Identifier



Note — The 5620 SAM uses the Hardware Identifier and Active Management IP parameters to help identify an eNodeB and resolve potential conflicts in the network.

- 9 Perform one of the following:
 - a If you have a eNodeB software upgrade policy that you need to use as a software upgrade override or you need to create one, go to step 10.
 - b If you do not need to use a software upgrade override for this pre-provisioned NE instance, go to step 14.
- 10 Perform one of the following:
 - a Choose an eNodeB software upgrade policy:
 - i Click on the Select button in the Software Upgrade Override panel. The Select Software Upgrade Policy form opens.
 - ii Configure the filter criteria, if required, and click on the Search button. A list of eNodeB software upgrade policies is displayed.
 - iii Choose an eNodeB software upgrade policy from the list and click on the OK button to return to the Pre-Provisioned NE form. Go to step 11.
 - b Create an eNodeB software upgrade policy:
 - i Click on the Select button in the Software Upgrade Override panel. The Select Software Upgrade Policy form opens.
 - ii Click on the Create button.
 - iii Perform Procedure 13-7.
 - iv When the new eNodeB software upgrade policy is created successfully, go to step 11.
- 11 Click on the Select button for the Image. The Select Software Image - Pre-Provisioned NE form opens.
- 12 Configure the filter criteria, if required, and click on the Search button. A list of eNodeB software images is displayed.
- 13 Choose a software image from the list and click on the OK button to close the form and return to the Pre-Provisioned NE form.

- 14 Click on the Apply button. The pre-provisioned NE instance is saved and created in the network. The 5620 SAM creates the Pre-Provisioned NEs equipment group if the group does not already exist. The form refreshes to display additional tabs.



Note — The 5620 SAM raises a warning alarm when you save a pre-provisioned NE instance without associating an NE WO with the instance.

- 15 Perform one of the following:

- a Associate an NE WO with the pre-provisioned NE instance.
 - i Click on the Activation tab button.
 - ii Click on the Select button. The Select NE Work Order form opens. A list of matching NE WOs is displayed.



Note — In order for an NE WO to appear in the Select NE Work Order form, the values that you entered for the Network Element ID and Network Element Version parameters must match the ENBEquipment *id* and NE version that are specified NE WO.

- iii Select an NE WO from the list and click on the OK button. The 5620 SAM automatically creates and starts an activation session to apply the NE WO.



Note 1 — If an existing activation session is already using the WO, the pre-provisioned NE instance does not create an activation session or apply the WO.

Note 2 — If an activation session remains in the started state for more than 24 h without being completed by an operator, an alarm is raised in the 5620 SAM.

- iv Click on the Apply button to save the pre-provisioned NE instance. A dialog box appears.
- v Click on the Yes button to close the dialog box.
- vi Close the Pre-Provisioned NE Manager form.
- b Close the Pre-Provisioned NE form without associating an NE WO.

Procedure 5-3 To delete a pre-provisioned NE instance

- 1 Choose Administration→Pre-Provisioned NE Manager from the 5620 SAM main menu. The Pre-Provisioned NE Manager form opens.
- 2 Configure the filter criteria, if required, and click on the Search button. A list of pre-provisioned NE instances is displayed.

- 3 Select a pre-provisioned NE instance from the list and click on the Delete button. A dialog box appears.
 - 4 Click on the Yes button. The pre-provisioned NE instance is deleted.
 - 5 Close the Pre-Provisioned NE Manager form.
-

Procedure 5-4 To delete the ENBEquipment object of a pre-provisioned NE instance

Deleting the ENBEquipment object erases the configuration data and allows you to bind another NE WO to the pre-provisioned NE instance.



Note — You cannot delete the ENBEquipment object of a managed eNodeB.

- 1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
 - 2 Click on the plus sign for the Pre-Provisioned NEs group and navigate to a pre-provisioned NE instance.
 - 3 Right-click on a pre-provisioned NE instance and choose Properties from the contextual menu. The Network Element form opens with the General tab displayed.
 - 4 Click on the Delete button in the ENB Base Configuration panel. A dialog box appears.
 - 5 Select the check box and click on the Yes button. The ENBEquipment object is deleted.
 - 6 Close the Network Element form.
-

5.5 eNodeB discovery

Procedure 5-5 describes how to create a mediation security policy and an SNMPv3 user, which are required for eNodeB discovery by the 5620 SAM and for SNMP communication. Procedure 5-6 describes how to create a discovery rules for eNodeBs that are intended for self-configuration, and offline and online configuration. See the *5620 SAM Parameter Guide* for descriptions of the parameters in the following procedures.

eNodeB discovery procedures

Perform the following procedures to configure the policies and object required for eNodeB discovery, and to discover an eNodeB using the 5620 SAM device discovery function.

Procedure 5-5 To configure the 5620 SAM to communicate with the eNodeB using SNMPv3

The following procedure describes the configuration of an SNMPv3 user and mediation policy intended specifically for 5620 SAM communication with the eNodeB. See the *5620 SAM User Guide* for more information about configuring a mediation policy.



Note — The eNodeB requires specific settings to be configured in the 5620 SAM in order for SNMP communication to occur. A mediation security policy and an NE user intended specifically for eNodeB management must be created. The following conditions must be met:

- The user name of the NE user specified in the mediation security policy is *initial_snm*.
- The password used in the password fields for the *initial_snm* user must match the password hard-coded on the eNodeB.
- The SNMP port is 161.
- The NetConf port is 830.
- The SNMP version is SNMPv3.

- 1 Create an NE user with SNMPv3 enabled on the 5620 SAM.
 - i Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.
 - ii Click on the Create button. The NE User, Global Policy (Create) form opens with the General tab displayed.
 - iii Enter *initial_snm* in the User Name field.
 - iv Enter a value for the Additional ID parameter.



Note — You can create two or more NE users with identical values for the User Name parameter by setting the Additional ID parameter. This allows you to accommodate eNodeBs with specific NE user requirements, such as the type of privacy policy.

- v Enter a description in the Description field, if required.
 - vi Select the *snmp* parameter to enable SNMP for the user. The form refreshes to display the SNMPv3 tab.
 - vii Click on the SNMPv3 tab button.

viii Configure the parameters:

- Authentication Protocol
- Privacy Protocol



Note — The settings for the Authentication Protocol, Privacy Protocol, and associated password parameters must match the corresponding parameters on the eNodeB.

ix Configure the parameters, if required:

- New Authentication Password
- Confirm New Auth Password

x Configure the parameters, if required.

- New Privacy Password
- Confirm New Privacy Password

xi Click on the OK button to create the user and close the NE User form. The NE user that you created is displayed in the NE User (NE Security) list.

xii Close the NE User Configuration form.

2 Configure an SNMPv3 mediation security policy on the 5620 SAM.

i Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

ii Click on the Mediation Security tab button.

iii Click on the Create button to create a new mediation security policy. The Mediation Policy (Create) form opens.

iv Enter a name for the mediation policy in the Displayed Name field.

v Choose SNMPv3(USM) from the Security Model drop-down menu. The SNMPv3 panel is displayed.

vi In the SNMP panel, set the Port parameter to 161, if required.

vii In the SNMPv3 panel, click on the Select button for the SNMPv3 user. The Select User form opens.

viii Choose the NE user you created in step 1 and click on the OK button to close the Select User form.

ix In the File Transfer panel, configure the File Transfer Type using the drop-down menu.

- x If you selected FTP for the File Transfer Type parameter, configure the following parameters in the FTP panel:
 - User Name
 - User Password
 - Confirm Password
 - Connect Timeout (sec)
 - Read Timeout (sec)



Note — In order to perform eNodeB software upgrades using the 5620 SAM, FTP or SFTP must be configured.

- xi If you selected Secure for the File Transfer Type parameter, configure the following parameters in the Secure FTP panel:
 - Connect Timeout (sec)
 - Read Timeout (sec)
- xii In the NETCONF panel:
 - Enter *initial_snm* in the User Name field.
 - Configure the User Password and Confirm Password fields.
 - Enter 830 in the Port field, if required.
- xiii Click on the OK button to close the Mediation (Create) form. A dialog box appears.
- xiv Click on the OK button to close the dialog box.
- xv Click on the OK button to close the Mediation (Edit) form and save the mediation security policy.

Procedure 5-6 To create a discovery rule for eNodeB management by the 5620 SAM

The 5620 SAM discovers devices by scanning the network as specified by the discovery rules. After a device is discovered, the 5620 SAM servers sets the device to a managed state and adds the device elements to the 5620 SAM database.

Follow the prompts provided to create a discovery rule intended for self-configuration, or offline/online configuration without self-configuration. See the *5620 SAM User Guide* more information about configuring discovery rules.



Note 1 — Discovery rules for self-configuration require specific settings that apply to self-configuration only.

Note 2 — An eNodeB can only be managed by one 5620 SAM server, or one set of redundant active and standby servers, at a time.

- 1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.
- 2 Click on the Create button. The Create Discovery Rule form opens.
- 3 To complete the Specify General Attributes step, perform the following steps:
 - i Configure the parameters:
 - Description
 - Administrative State
 - OLC State
 - Management Protocol
 - ii Click on the Select button for the Group Name. The Select Discovery Group form opens.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of discovery groups is displayed.



Note — The Pre-Provisioned NEs group does not display if no pre-provisioned NE instances exist. Perform Procedure 5-2 to create a pre-provisioned NE instance.

- iv Select a group from the list and click on the OK button. The Select Discovery Group form closes.
 - v Click on the Next Button.
- 4 To complete the Add Rule Elements step, perform the following steps:
 - i Click on the Create button. The Topology Discovery Rule Element (Create) form opens.
 - ii Configure the parameters:
 - IP Address
 - Mask Bits
 - Usage



Note — Alcatel-Lucent recommends using IP address ranges, rather than individual IP addresses, as rule elements for eNodeB discovery.

- iii Click on the Apply button. The rule element is added to the discovery rule.
 - iv Repeat substeps ii and iii to add more rule elements to the discovery rule, as required.
 - v Click on the Cancel button or the close button. The Topology Discovery Rule Element (Create) form closes.
 - vi Click on the Next button. The Add Auto Discovery Rule Elements ACL step does not apply to eNodeB management.
 - vii Click on the Next button.
- 5 To complete the Configure Mediation Security step, perform the following steps:
- i Click on the Select button in the Read Access Mediation Policy panel. The Configure Mediation Security form opens.
 - ii Select the mediation security policy that you created in Procedure 5-5 from the list and click on the OK button.
 - iii Click on the Select button in the Write Access Mediation Policy panel. The Configure Mediation Security form opens.
 - iv Select the mediation security policy that you created in Procedure 5-5 from the list and click on the OK button.
 - v Click on the Select button in the Trap Access Mediation Policy panel. The Configure Mediation Security form opens.
 - vi Select the mediation security policy that you created in Procedure 5-5 from the list and click on the OK button.
 - vii Click on the Next button.
- 6 To complete the Configure Management Ping Policy step, perform the following steps:



Note — This step of the Create Discovery Rule process is only required if you have created a custom ping policy and want to assign it to the eNodeBs that will be discovered by this discovery rule.

- i Click on the Select button in the Out Of Band Management Interface Ping panel. The Configure Management Ping Policy form opens.
- ii Select a ping policy from the list and click on the OK button.
- iii Click on the Select button in the In Band Management Interface Ping panel. The Configure Management Ping Policy form opens.
- iv Select a ping policy from the list and click on the OK button.
- v Click on the Next button.

- 7 To complete the Configure MIB Statistics Policy step, perform the following steps:
 - i Click on the Select button. The Configure MIB Statistics Policy form opens.
 - ii Select a MIB statistics policy from the list and click on the OK button.
 - iii Click on the Next button.
- 8 To complete the Add Discovered Routers to Span(s) step, perform the following steps:
 - Click on the Add button. The Select Span(s) form opens.
 - Choose a span from the list and click on the OK button.
 - Click on the Next button.
- 9 To complete the Configure Backup Policy step, perform the following steps:
 - i Click on the Select button. The Select Backup Policy form opens.
 - ii Choose a RAN based backup policy from the list and click on the OK button.
 - iii Click on the Next button.
- 10 In the Add NE Self Config Policies step, perform one of the following:
 - a If you are creating a discovery rule for self-configuration:
 - i Click on the Add button. The Select form opens.
 - ii Configure the filter criteria, if required, and click on the Search button. A list of NE self-configuration policies is displayed.
 - iii Choose the NE self-configuration policy that you created in Procedure 5-1 and click on the OK button to close the form.
 - b If you are creating a discovery rule that will not be used to discover eNodeBs intended for self-configuration, go to step 11.
- 11 Click on the Finish button to close the Create Discovery rule form.
- 12 Click on the Apply button in the Discovery Manager form. A dialog box appears.



Note — You can only choose one NE self-configuration policy for a device type.

- iv Click on the Next button.

- 13 Click on the Yes button to close the dialog box. The discovery rule that you created in this procedure is saved and activated.



Note 1 – The discovery rule that you created in this procedure is not saved or activated until you click on the OK button or the Apply button in the containing Discovery Manager form and confirm the system changes.

Note 2 – Discovery rules that are shut down are not applied.

- 14 Perform the following, as required:
 - a Perform Procedure 5-8 to run the self-configuration process flow when the 5620 SAM discovers eNodeBs intended for self-configuration.
 - b Perform Procedure 5-9 to manage eNodeB discovery for online configuration.
-

Procedure 5-7 To view and sort the deployment status of pre-provisioned NE instances

Perform this procedure to sort pre-provisioned NE instances by their deployment status and access the Properties form of an instance. Perform Procedure 5-8 to run the self-configuration process flow of a pre-provisioned NE instance.

- 1 Choose Administration→Pre-Provisioned NE Manager from the 5620 SAM main menu. The Pre-Provisioned NE Manager form opens.
 - 2 Click on the drop-down menu at the top left corner of the form and choose Pre-Provisioned NE Status (Self Config). The form refreshes and displays additional filter options.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of pre-provisioned NE instances is displayed.
 - 4 Configure the filter criteria in one or more columns of the main panel and click on the Search button. A list of pre-provisioned NE instances is displayed based on the defined filter criteria.
 - 5 Choose a pre-provisioned NE instance from the list and click on the Properties button. The Pre-Provisioned NE Status form opens.
 - 6 Perform configuration tasks as required.
-

Procedure 5-8 To run the self-configuration process flow for a pre-provisioned NE instance that has a status of Detected Node

Perform this procedure to verify the discovery status of a pre-provisioned NE instance and run the configuration process flow when checkpoints are enabled on the instance.



Caution — The configuration deployment phase of self-configuration overwrites the entire eNodeB NetConf object tree. You erase all prior configuration on the eNodeB when you run the self-configuration process flow.



Note — This procedure is required only when checkpoints are enabled in the self-configuration policy. The process flow runs automatically when checkpoints are not enabled.

- 1 Choose Administration→Pre-Provisioned NE Manager from the 5620 SAM main menu. The Pre-Provisioned NE Manager form opens.
 - 2 Choose Pre-Provisioned NE Status (Self Config) from the object drop-down list. The form refreshes to display additional state and parameter columns.
 - 3 Configure the filter criteria for the State column to filter on a state of Detected Node and click on the Search button. A list of pre-provisioned NE instances with a State of Detected Node is displayed.
 - 4 Select a pre-provisioned NE instance from the list and click on the Properties button. The Pre-Provisioned NE Status form opens.
 - 5 Click on the Continue button to initiate a step of the process flow. A dialog box appears.
 - 6 Select the check box click on the OK button. A check mark appears beside the step of the process flow that is now complete.
 - 7 Repeat steps 5 and 6 until the process flow is complete.
 - 8 Click on the OK button or Cancel button to close the Pre-Provisioned NE form.
-

Procedure 5-9 To manage the discovery of an eNodeB

Perform this procedure to discover devices by scanning the network, as specified in the discovery rules.

See the *5620 SAM User Guide* for more information about tasks you can perform with newly discovered devices.

- 1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.
- 2 Click on the Managed State tab button. A list of discovered devices displays.

- 3 Configure the filter criteria, if required, and click on the Search button. A list of discovered devices is displayed.
- 4 Verify that eNodeBs are discovered and managed.
- 5 Perform the following steps, as required.
 - a Click on the Manage button to set unmanaged eNodeBs to managed.
 - b Performing Procedure 5-11 to set an identifier for unidentified eNodeBs, as required.
 - c Ping management IP addresses. See Procedure 5-10 for more information.
- 6 Perform the following steps to move a discovered eNodeB from the Discovered NEs group to the Network group, if required.



Note — This step is required if the discovery rule specifies the Discovered NEs group as the Group Name. See step 3 of Procedure 5-6 for more information.

- i In the Physical Topology window, click on the Discovered NEs group. The Discovered NEs form opens.
- ii Select one or more eNodeBs from the list and drag and drop them to the network icon in the equipment view of the navigation tree or to the topology map, as required.

Procedure 5-10 To ping an eNodeB

The 5620 SAM uses ICMP to ping eNodeBs. Unless specified otherwise in the discovery rule, eNodeBs are added to the default ping policy when the NEs are discovered by the 5620 SAM. See the *5620 SAM User Guide* for more information about ping policies.



Note — The 5620 SAM raises the InBandManagementConnectionDown alarm when an NE cannot be pinged.

- 1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.
- 2 Click on the Ping tab button.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of ping policies is displayed.
- 4 Select a ping policy from the list and click on the Properties button. The Management Ping Policy (Edit) form opens with the General tab displayed.
- 5 Click on the Ping Destinations tab button.

- 6 Select one or more NEs from the list. To select multiple NEs, hold down the CTRL button and click.
 - 7 Click on the Ping button. The 5620 SAM attempts to ping the NEs.
 - 8 Verify the status of the ping attempt in the Status column. The status displays as Success when the ping is successful.
 - 9 Close the Management Ping Policy (Edit) form.
 - 10 Close the Mediation (Edit) form.
-

Unidentified eNodeBs

The 5620 SAM uses the value of the ENBEquipment id parameter as the identifier for the device in the network. Any eNodeBs without a value entered for this parameter are not fully discovered by the 5620 SAM until a value is entered.

Perform Procedure 5-11 to enter a value for the id parameter of the ENBEquipment object.

Procedure 5-11 To enter a value for an unset id parameter for an eNodeB

The UnidentifiedNode alarm should be visible before you perform this procedure.

- 1 Perform one of the following:
 - a Use the UnidentifiedNode alarm to access the device.
 - i Choose Window→Alarm Window from the 5620 SAM main menu.
 - ii Right-click on the UnidentifiedNode alarm and choose Show Affected Object from the contextual menu. The Discovered Node form opens with the General tab displayed.
 - b Use the discovery manager to access the device.
 - i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.
 - ii Choose the discovery rule that caused the discovery of the unidentified device from the list and click on the Properties button. The Topology Discovery Rule form opens with the General tab displayed.
 - iii Click on the Discovered Nodes tab button.
 - iv Choose the unidentified device from the list and click on the Properties button. The Discovered Node form opens with the General tab displayed.

- 2 Configure the Network Element ID parameter.
- 3 Click on the OK button to close the Discovered Node form.

The eNodeB moves to the intended group in the navigation tree and topology map. The 5620 SAM uses the value entered in step 2 as the identifier for the device.

5.6 Unmanaging and deleting eNodeBs from the 5620 SAM network

The process for unmanaging and deleting an eNodeB is the same as for other NE types. You cannot use a WO to delete an eNodeB from the 5620 SAM managed network. Unmanaging and deleting a device results in a loss of management data for the device.

Procedure 5-12 To unmanage and delete an eNodeB



Warning — Unmanaging and deleting an NE results in a loss of management data and completely removes the NE from the managed network. See the *5620 SAM User Guide* for more information.

- 1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the General tab displayed.
 - 2 Click on the Managed State tab button.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of managed NEs is displayed.
 - 4 Select an eNodeB from the list.
 - 5 Choose one of the following:
 - a If the eNodeB is currently managed:
 - i Click on the Unmanage button. A dialog box appears.
 - ii Click on the Yes button.
 - iii Wait for the state to change to Unmanaged. Go to step 6.
 - b If the eNodeB is currently unmanaged, go to step 6.
 - 6 Click on the Delete button. A dialog box appears.
 - 7 Click on the Yes button. The eNodeB is deleted by the 5620 SAM.
-

6 — eNodeB offline configuration

- 6.1 Offline configuration overview 6-2**
- 6.2 Workflow to manage offline configuration 6-3**
- 6.3 Activation manager 6-4**
- 6.4 Configuration snapshots 6-11**
- 6.5 WO and configuration snapshot file management 6-18**

6.1 Offline configuration overview

Offline configuration is the process of managing CM XML files in order to deploy configuration data to and retrieve configuration data from eNodeBs. You can manage CM XML workorder and configuration snapshot files using the 5620 SAM.

Workorders

A workorder (WO) is a CM XML file that creates or modifies eNodeB parameter objects when the file is deployed to the device using the 5620 SAM. WOs have a file extension of .xwo. WOs in the 5620 SAM server are located in the *installation_directory/activation/wo_import* directory, where *installation_directory* is the 5620 SAM base directory, typically /opt/5620sam/server/nms/.

You can deploy WO files using the 5620 SAM activation manager and complete the following tasks:

- create or delete pre-provisioned NE instances
- configure managed eNodeBs



Note — You cannot deploy a WO to unmanage an eNodeB or delete a managed eNodeB from the 5620 SAM network.

Code 6-1 describes the XML structure of a WO.

Code 6-1: Sample WO and contained NE WO

```
<?xml version="1.0" encoding="UTF-8"?>
<workorders>
  <workorder name="sample NE WO" creationDate="2011-10-26 16:20:07.533
+0200" originator="admin" description="none">
    <ENBEquipment id="eNB101" model="ENB" version="LA_04_00"
method="create">
      <attributes>
        workorder content
      </attributes>
    </workorder>
  </workorders>
```

The 5620 SAM creates WO import logs that contain information and warnings. Perform Procedure 6-10 to view WO import logs.

Activation sessions and the activation manager

The activation manager is the function in the 5620 SAM for managing WO deployment. You can use the activation manager to perform the following tasks:

- validate WO files and detect errors
- acquire configuration locks on eNodeBs to prevent conflicting configuration
- deploy WO files to eNodeBs

- fallback WO deployment to correct device or network errors that occur as a result of WO deployment
- schedule WO deployment within a 24 h time window

See section 6.3 for more information about using the activation manager.

Configuration snapshots

You can use configuration snapshots to capture CM XML snapshot files of eNodeB NE configurations in the 5620 SAM network. You can use configuration snapshot files for the following purposes:

- To reuse proven eNodeB configuration settings and create new WO files for deployment to other eNodeBs.
- To provide the 9959 NPO with up-to-date information on eNodeB configuration and status for planning and network optimization.
- To back up eNodeB gamma parameter configuration in conjunction with a backup/restore policy. See chapter 13 for more information about the backup/restore function of the 5620 SAM.

You must schedule a daily, recurring configuration snapshot of all managed eNodeBs in order to provide a complete image of the network to the NPO. See section 6.4 for more information about configuration snapshots.

6.2 Workflow to manage offline configuration

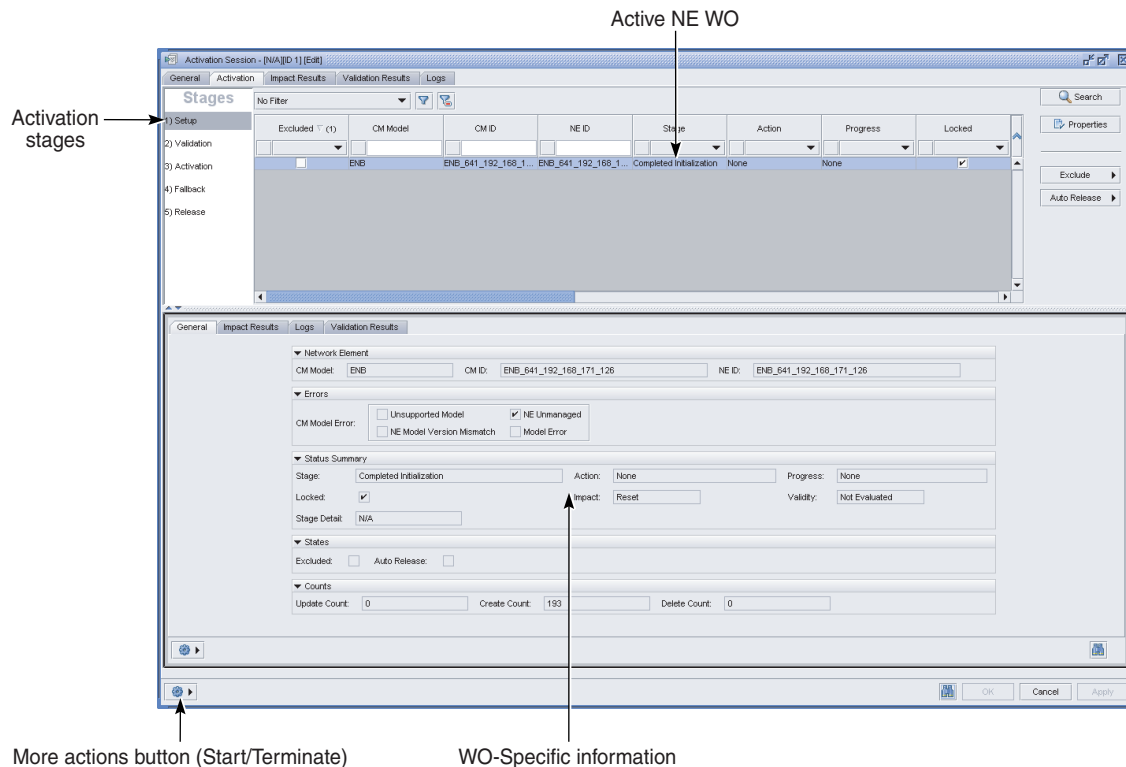
- 1 Use the 9952 WPS to create WO files containing configuration data for eNodeBs, and transfer the files to the 5620 SAM, as required.
- 2 Use the 5620 SAM activation manager function to validate and deploy WOs to eNodeBs.
 - i Create an activation session. See Procedure 6-1.
 - ii Deploy a WO using the activation manager. See Procedure 6-2.
 - iii Delete activation sessions, as required. See Procedure 6-3.
- 3 Use the 5620 SAM configuration snapshot function to export eNodeB configuration data in the form of snapshot files.
 - i Create a snapshot instance. See Procedure 6-4.
 - ii Take manual configuration snapshots. See Procedure 6-5.
 - iii Create a schedule for single or recurring configuration snapshots. See Procedure 6-6.

- 4 Automatically or manually transfer snapshot files to the following application server types:
 - 9952 WPS
 - 9959 NPO
- 5 Perform file management tasks for CM XML files and activation log files.
 - i Configure WO and configuration snapshot disk usage in the nms-server.xml file, as required. See Procedure 6-8.
 - ii Delete WO files from the 5620 SAM main server file system. See Procedure 6-9.
 - iii View and delete WO import logs, as required. See Procedures 6-10 and 6-11.
 - iv Configure the default size constraint policy for WO import logs, as required. See Procedure 6-12.

6.3 Activation manager

The activation manager is the 5620 SAM function for deploying a WO to an eNodeB. See Figure 6-1 for an example of a started activation session that is ready to deploy a WO. The WO contains a single NE WO for the purpose of creating a pre-provisioned NE profile.

Figure 6-1 Activation session



22491

Running an activation session

You must create an activation session before you can use the activation manager to deploy a WO. Perform Procedure 6-1 to create an activation session.

An activation session acquires a configuration lock for the target eNodeBs when an operator, or the 5620 SAM, starts the session. Configuration locks prevent any changes outside of the activation session from being applied to the eNodeBs in order to prevent device configuration conflicts. Configuration locks can be released when an operator terminates the activation session, in the Release stage, and by the auto-release function.

If two or more activation sessions attempt to acquire a configuration lock on the same eNodeB, only the first lock attempt succeeds. Subsequent configuration lock attempts by activation sessions display the lock status as Waiting.

Once started, an activation session can be scheduled for automatic execution up to 24 hours in the future. Activation sessions waiting to be executed by the scheduler remain in the started state, and all associated eNodeBs remain locked until the session execution is completed.



Note 1 — Only one WO can be associated with an activation session at a time. A WO can only be associated with one activation session at a time.

Note 2 — The maximum number of started activation sessions is 5.

The activation manager notifies operators when the activation of a WO will affect network license tokens. The 5620 SAM blocks WO activation when there is a RAN license violation in the managed network. WO activation is permitted when you import a new license file that contains a sufficient amount of license entitlement capacity to resolve the license violation. WO fallback is permitted by the 5620 SAM even when the fallback operation will result in a license violation.

When an activation session is loaded into the activation manager, you can start the session to acquire device configuration locks and perform the following stages in sequence:

- 1 Setup: loads the WO and performs an XML sanity check.
- 2 Validation: runs validation checks on NE WOs.
- 3 Activation: deploys the NE WOs to the applicable eNodeBs.
- 4 Fallback: reverts configuration changes, if required, undoing the Activation stage.
- 5 Release: releases configuration locks.

At any stage in the activation process, you can view activation logs, validation errors, and the XML structure of the active WO. Perform Procedure 6-2 to deploy a WO to an eNodeB using the activation manager.

Activation manager procedures

Perform the procedures in this section to deploy WOs to discovered and managed eNodeBs using the activation manager, and to create pre-provisioned NE instances by activating WOs for which there is no corresponding discovered eNodeB. See the *5620 SAM Parameter Guide* for descriptions of the parameters in the following procedures.

Procedure 6-1 To create an activation session

Perform this procedure to create an activation session for WO deployment in the activation manager.

- 1 Choose Manage→Mobile Access→Activation from the 5620 SAM main menu. The Activation form opens.
 - 2 Choose Activation Session (Activation) from the object drop-down list, if required.
 - 3 Click on the Create Activation Session button. The Activation Session (Create) form opens.
 - 4 Configure the parameters:
 - Name
 - Description
 - 5 Click on the OK button to save the activation session and close the Activation Session (Create) form.
-

Procedure 6-2 To deploy a WO using the activation manager

Perform this procedure to deploy a WO and any contained NE WOs to the 5620 SAM network. The following conditions must be true in order to deploy an NE WO:

- You have a 5620 SAM user account with an Administrator or Work Order Activation scope of command role.
- The NE WO corresponds to a managed eNodeB, or the NE WO contains a complete set of valid objects for creating a new pre-provisioned NE profile.
- The NE WO is in the supported CM XML format and does not contain model errors.
- The NE version specified in the NE WO is supported by the 5620 SAM.
- There are no RAN license violations in the 5620 SAM network.
- The NE WO successfully passes the Validation stage of the activation process.



Caution — When you deploy an NE WO to a managed eNodeB, a full or partial reset of the device can occur, which is service-affecting.

- 1 Choose Manage→Mobile Access→Activation from the 5620 SAM main menu. The Activation form opens.
- 2 Choose Activation Session (Activation) from the object drop-down list, if required.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of activation sessions is displayed.
- 4 Select an activation session from the list and click on the Properties button. The Activation Session (Edit) form opens with the General tab displayed.
- 5 In the Associated Work Orders panel, click on the Add button. The Add form opens.
- 6 Configure the filter criteria, if required, and click on the Search button. A list of applicable WOs is displayed.
- 7 Select a WO from the list and click on the OK button to close the Add form. The WO is associated with the current activation session.



Note — A WO that is associated with an activation session cannot be deleted from the session.

- 8 Click on the Activation tab button. The Setup stage is selected by default in the Stages panel. NE WOs are displayed as a list.

- 9 Complete the Setup stage of the activation session.
 - i Select one or more NE WOs from the list and click on the Exclude button to exclude or re-include NE WOs from deployment, as required.
 - ii Click on the More Actions button and choose Start Session. The 5620 SAM evaluates the model, impact, and device management status of each NE WO.



Note 1 — When an activation session starts, the 5620 SAM acquires configuration locks on managed eNodeBs that will be impacted by NE WO deployment. The 5620 SAM releases the configuration locks when an operator terminates the activation session.

Note 2 — NE WOs with CM Model errors are not passed into the Activation stage, and cannot be deployed.

Note 3 — The 5620 SAM raises an alarm if an activation session has a Status of Active for more than 24 h.

- iii Verify that the Completed Initialization message appears in the Stage column for each NE WO in the list.
 - iv Click on the Auto Release button to enable or disable automatic release of configuration locks at the end of the Activation stage, as required.



Caution — When you enable auto-release, the Fallback stage cannot be performed.

- v Click on the Impact Results tab button and verify device impact, as required.
 - vi Click on the Logs tab button and view log messages, as required.
 - vii In the Stages panel, click on the Validation button. NE WOs that have successfully passed the Setup stage are displayed.
- 10 Complete the Validation stage of the activation session.
 - i Select an NE WO from the list and click on the Validate button. To select multiple NE WOs for simultaneous validation, hold down the Shift or CTRL keys while clicking on NE WOs.
 - ii Click on the Validation Results tab button.
 - iii Click on the Search button. A list of errors and warnings associated with the validated NE WOs is displayed. The NE WOs are valid if no faults appear in the Validation Result panel.



Note 1 — Validation results are only displayed for NE WOs that have been validated.

Note 2 — You cannot deploy an NE WO that has not been validated.

- 11 Click on the Schedule button to set WO deployment to be executed automatically, up to 24 h later, if required. See the *5620 SAM User Guide* for information about using the 5620 SAM scheduler.
- 12 Perform one of the following:
 - a If no serious errors are identified in NE WOs during the Validation stage, click on the Activation button in the Stages panel and go to step 13.
 - b If faults are identified in NE WOs during the Validation stage:
 - i Resolve the issue that is preventing WO deployment. The following actions are examples only.
 - In the case of CM model errors, choose or create a WO that does not contain CM model errors.
 - In the case of RAN license errors, perform Procedure 9-1 to import RAN license capacity into the 5620 SAM network.
 - Exclude NE WOs, as required, and go to 13 to continue the activation process for valid NE WOs.
 - ii Click on the More Actions button and choose Terminate Session. Configuration locks are released.
 - iii Delete the current activation session.
 - iv Perform Procedure 6-1 to create a new activation session.
 - v Perform this procedure again.
- 13 Complete the Activation stage of the activation session.



Caution — The deployment of WOs to active devices may be service-affecting.

- i Evaluate the possible consequences of WO deployment, including:
 - full or partial device resets and resulting service interruption
 - consumption of RAN license entitlement tokens
 - available system resources of the 5620 SAM, particularly for WOs that contain multiple NE WOs
 - auto-release settings and the inability to fallback after a configuration lock release occurs
- ii Select an NE WO from the list and click on the Activate button. To select multiple NE WOs for simultaneous activation, hold down the Shift or CTRL keys while clicking on NE WOs.
- iii Verify the messages as they appear in the Stage, Action, and Progress columns.
- iv Click on the Logs tab button and view log messages, as required.

- 14 Perform one of the following.
 - a If you must undo the configuration changes that have been caused by the Activation stage, go to step 15 and perform the Fallback stage.
 - b If the Activation stage is successful and you want to finalize the configuration changes, go to step 16.
- 15 Complete the Fallback stage of the activation session, if required.



Caution — Fallback of WO deployment can be service-affecting.



Note 1 — Perform this step only if you need to undo the changes caused by the WO deployment and return the eNodeBs to their pre-existing configurations.

Note 2 — You cannot perform a fallback on an eNodeB when the activation session is terminated and the configuration lock is released.

- i Select an NE WO from the list and click on the Fallback button. To select multiple NE WOs for simultaneous fallback, hold down the Shift or CTRL keys while clicking on NE WOs.
 - ii In the bottom half of the Activation Session form, click on the General tab button.
 - iii Verify that the fallback has been performed successfully.
 - iv Click on the Terminate Session button to release the configuration locks.
 - v Delete the current activation session to deploy another WO, if required.
 - vi Perform Procedure 6-1 to create another activation session, if required.
 - vii Repeat this procedure with a different WO, or exclude eNodeBs from the activation session as required.
- 16 Perform one of the following.
 - a If auto-release is enabled, go to step 18.
 - b If auto-release is disabled, go to step 17.

- 17 Complete the Release stage of the activation session.
 - i Verify that a fallback is not required.
 - ii Select an NE WO from the list and click on the Release button. To select multiple NE WOs for simultaneous release, hold down the Shift or CTRL keys while clicking on NE WOs.
 - iii Go to step 18.
 - 18 Click on the More Actions button and choose Terminate Session. The activation session stops and the configuration locks are released.
-

Procedure 6-3 To delete an activation session



Note — You must terminate the activation session if the session status is Active.

- 1 Choose Manage→Mobile Access→Activation from the 5620 SAM main menu. The Activation form opens.
 - 2 Choose Activation Session (Activation) from the object drop-down list, if required.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of activation sessions is displayed.
 - 4 Select an activation session from the list and click on the Delete button. A dialog box appears.
 - 5 Click on the Yes button. The activation session is deleted.
 - 6 Close the Activation form.
-

6.4 Configuration snapshots

Configuration snapshots are CM XML files with a .xcm file extension that are generated by the 5620 SAM to capture the parameter configuration of one or more managed eNodeBs or pre-provisioned NE profiles. You can specify a list of eNodeBs that will be included in a configuration snapshot, or you can use inclusion filters to dynamically include eNodeBs based on criteria such as Site ID.

Configuration snapshots are stored in the *installation_directory/nms/activation/snapshot_export* directory, where *installation_directory* is the 5620 SAM base directory.

Configuration snapshot files are named with the following convention:

snapshot-snapshot_instance-datestamp-ID.xcm.gz

where

snapshot_instance is the name of the snapshot instance that generated the file

timestamp is the date in YYYY-MM-DD-HH-MM-SS format

ID is the ID number of the snapshot

.gz is the extension when the 5620 SAM is configured to compress the snapshot file using Gzip

You can use the 9952 WPS to convert a configuration snapshot into a WO. This function facilitates eNodeB provisioning by allowing you to reuse proven device parameter settings and apply them to other eNodeBs or pre-provisioned NE instances via offline configuration. When creating a snapshot instance and configuration snapshots for export to the 9952 WPS, you must configure the snapshot instance specifically for that purpose.

The 9959 NPO requires daily configuration snapshots of the RAN as managed by the 5620 SAM. A daily snapshot provides the NPO with an updated representation of both the planned and currently managed RAN so that to NPO operators can successfully optimize device parameter settings for the 5620 SAM network. When creating a snapshot instance and configuration snapshots for export to the 9959 NPO, you must configure the snapshot instance specifically for that purpose.

Configuration snapshot procedures

Perform the following procedures to manage configuration snapshots for eNodeBs.

Procedure 6-4 To create a snapshot instance

Perform this procedure to create a snapshot instance that is intended to do one of the following tasks:

- capture the configuration of all eNodeBs in the network, which is generally performed for use with the 9959 NPO
 - capture the configuration of a single eNodeB, which is generally performed for use with the 9952 WPS
 - capture the configuration of a subset of eNodeBs
- 1 Choose Manage→Mobile Access→Snapshot Instances from the 5620 SAM main menu. The Snapshot Manager form opens.
 - 2 Click on the Create button. The Snapshot (Create) form opens with the General tab displayed.
 - 3 Configure the parameters:
 - Snapshot Name
 - Description

4 Configure the parameters in the Filtering and Snapshot File Format panels:

- Include Components and Attributes with Manufacturer Visibility
- Include States and Statuses
- Include Attributes with Read-Only Access
- Include Additional Information Attributes
- Include in the snapshot
- Gzip Exported File



Note — You must select all of the check boxes in the Filtering panel and choose All Entities in the Network from the Include in the snapshot drop-down list to take a configuration snapshot of all eNodeBs for use with the 9959 NPO. You must deselect all of the check boxes in the Filtering panel and choose NE Entities Only from the Include in the snapshot parameter drop-down list to take a configuration snapshot for use with the 9952 WPS.

5 Choose one of the following:

- a If you selected All Entities in the Network for the Include in the snapshot parameter, go to step 13.
- b If you selected NE Entities Only for the Include in the snapshot parameter, go to step 8.
- c If you selected Inclusion Filters Only for the Include in the snapshot parameter, go to step 6.

6 To apply an inclusion filter which is already configured, perform the following steps, if required:

- i Click on the Inclusion Filters tab button.
- ii Click on the Add button. The Select form appears.
- iii Configure the filter criteria, if required, and click on the Search button. A list of available inclusion filters is displayed.
- iv Select one or more inclusion filters from the list. To select multiple inclusion filters, hold down the CTRL key and click on the inclusion filters. Click on the OK button to close the Select form.

7 To create and apply a new inclusion filter, perform the following steps, if required:

- i Click on the Inclusion Filters tab button.
- ii Click on the More Actions button and choose Inclusion Filters Creation. The Inclusion Filters Creation form opens.
- iii Choose Network Element (Network) from the drop-down menu.
- iv Click on the Filter button. The Inclusion Filters Creation - Filter form opens.
- v Choose an attribute from the Attribute drop-down menu.
- vi Choose a function from the Function drop-down menu.

- vii Configure the Value parameter.
 - viii Click on the Add button. The entry is added to the filter.
 - ix Repeat steps v to viii to configure additional filter entries, as required.
 - x Click on the Save button. The Save Filter form appears.
 - xi Configure the following parameters:
 - Filter Name
 - Description
 - Public
 - xii Click on the Save button. The Save Filter form closes and the filter is saved.
 - xiii Click on the Apply button. The filter is applied to the Inclusion Filters Creation form and eNodeBs that match the filter are displayed in the Inclusion Filters Creation form.
 - xiv Click on the Close button to close the Inclusion Filters Creation - Filter form.
 - xv Verify that one or more NEs are displayed in the Inclusion Filters Creation form, if required.
 - xvi Close the Inclusion Filters Creation form and return to the Snapshot (Create) form.
 - xvii Click on the Add button. The Select form opens.
 - xviii Configure the filter criteria, if required, and click on the Search button. A list of inclusion filters is displayed.
 - xix Select an inclusion filter from the list and click on the OK button. The Select form closes and the inclusion filter is displayed in the Snapshot (Create) form.
 - xx Go to step 13.
- 8 Click on the NE Entities tab button.
 - 9 Click on the Add button. The Add form opens.
 - 10 Configure the filter criteria, if required, and click on the Search button. A list of eNodeBs is displayed.
 - 11 Select one or more eNodeBs from the list. To select multiple eNodeBs, hold down the CTRL key and click on the eNodeBs. Click on the OK button.

The eNodeBs that you selected are displayed in the Snapshot (Create) form.
 - 12 To delete an eNodeB from the snapshot instance, if required, select an eNodeB from the list and click on the Delete button.
 - 13 Click on the OK button to save the snapshot instance and close the Snapshot (Create) form.
-

Procedure 6-5 To take a configuration snapshot

You must configure a snapshot instance before you can take a configuration snapshot. See Procedure 6-4.



Note — When you successfully take a configuration snapshot that uses inclusion filters, the NEs that are included in the filters are added to the NE entities list.

- 1 Choose Manage→Mobile Access→Snapshot Instances from the 5620 SAM main menu. The Snapshot Manager form opens.
- 2 Configure the filter criteria, if required, and click on the Search button. A list of snapshot instances is displayed.
- 3 Select a snapshot instance from the list and click on the Properties button. The Snapshot (Edit) form opens with the General tab displayed.
- 4 Verify the parameters of the snapshot instance, as required.
- 5 Click on the More Actions button and choose Extract File.



Note — You can cancel a snapshot operation by clicking on the More Actions button and choosing Cancel Extract.

The state of the snapshot displays in the Snapshot State panel, including the following:

- the state of the most recent snapshot attempt (success or failure)
- the execution time of the most recently attempted snapshot
- the file name of the last successful snapshot

- 6 Click on the NE Entities tab button.
- 7 Verify the success of the snapshot for each NE by viewing the State column of the list.



Note — It is possible for the snapshot to fail for individual eNodeBs. Configuration data for eNodeBs that do not display Success in the State column is not included in the snapshot file.

- 8 Close the Snapshot (Edit) form.
-

Procedure 6-6 To schedule a configuration snapshot

A snapshot instance must include one or more eNodeBs before you can schedule the snapshot. You can schedule a snapshot to be taken once, or on an ongoing basis. See Procedure 6-4 for information about how to create a snapshot instance.

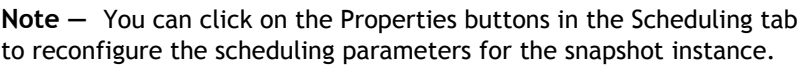
See the *5620 SAM User Guide* for more information about scheduling tasks using the 5620 SAM scheduler. See the *5620 SAM Parameter Guide* for more information about the scheduler parameters in this procedure.



Note — The 9959 NPO requires a configuration snapshot of all RAN devices in the network. Ensure that the Include in snapshot parameter is set to All Entities in the Network for the snapshot instance that you choose in step 3 of this procedure.

- 1 Choose Manage→Mobile Access→Snapshot Instances from the 5620 SAM main menu. The Snapshot Manager form opens.
- 2 Configure the filter criteria, if required, and click on the Search button. A list of snapshot instances is displayed.
- 3 Select a snapshot instance from the list and click on the Properties button. The Snapshot (Edit) form opens with the General tab displayed.
- 4 Click on the More Actions button and choose Schedule. The STM Scheduled Task (Create) form opens.
- 5 Configure the following parameters:
 - Scheduled Task Name
 - Scheduled Task Description
 - Administrative State
- 6 In the Schedule panel, click on the Select button. The Select Schedule form opens.
- 7 Perform one of the following:
 - a Create a daily, recurring schedule for the configuration snapshot.
 - i Click on the Create button. The SAM Schedule form opens with the General tab displayed.
 - ii In the Information panel, configure the following parameters:
 - Name
 - Description
 - Current Client Start Time
 - iii Select the Ongoing check box.
 - iv Choose Per Day from the Frequency drop-down list. The form refreshes to display additional parameters.
 - v Select the Run Every Day radio button in the Frequency Settings panel.
 - vi Click on the OK button to return to the Select Schedule form. The schedule that you created is displayed in the list.
 - vii Select a schedule from the list and click on the OK button to return to the STM Scheduled Task form. The schedule that you selected is applied to the scheduled task.
 - viii Click on the OK button to return to the Snapshot (Edit) form.

- 9 Verify that the schedule is correctly configured.



Procedure 6-7 To delete a snapshot instance

- 1 Choose Manage→Mobile Access→Snapshot Instances from the 5620 SAM main menu. The Snapshot Manager form opens.
 - 2 Configure the filter criteria, if required, and click on the Search button. A list of snapshot instances is displayed.
 - 3 Select a snapshot instance from the list and click on the Delete button. A dialog box appears.
 - 4 Click on the Yes button to delete the snapshot instance.
 - 5 Close the Snapshot Manager form.
-

6.5 WO and configuration snapshot file management

You can use the 5620 SAM to manage CM WO and snapshot files, log files, and server parameters for file management. You can configure file management parameters for WO and configuration snapshot files as well as WO import logs.

File transfer between the 5620 SAM and the 9952 WPS

You can set up the automatic transfer of CM XML files between the 5620 SAM and the 9952 WPS by enabling the live server repository function of the 9952 WPS. Manual transfer via FTP is also supported. See the *9952 WPS User Guide* for more information about the live server repository function.



Note — You must enable SSL on the 5620 SAM main server before you can use the live server repository function of the 9952 WPS to import and export CM XML files.

Activation parameters in nms-server.xml

The 5620 SAM manages WO and configuration snapshot files according to parameter settings that are specified in the nms-server.xml configuration file. See Code 6-2 for a listing of the parameters in the activation section of nms-server.xml. The values listed are the default values.

Code 6-2: Activation file management parameters

```
<activation
importDaysToKeep="7"
importMaxSizeInMb="10000"
importPercentToKeepAfterPurge="75"
importRaiseAlarmWhenSizeLeftInPartitionInMb="1000"
importSyncEnabled="true"
importSyncInterval="60"
numDbThreads="10"
snapshotExportsDaysToKeep="7"
snapshotExportsMaxSizeInMb="10000"
```

```

snapshotExportsPercentToKeepAfterPurge="75"
snapshotExportsRaiseAlarmWhenSizeLeftInPartitionInMb="1000"
snapshotExportsSyncEnabled="true"
snapshotExportsSyncInterval="60"
workingSyncEnabled="true"
workingSyncInterval="60" />

```

Parameters that are prefixed by *snapshotExports* specify file management settings for the *snapshot_export* directory. Parameters that are prefixed by *import* specify file management settings for the *wo_import* directory.

The following behaviors apply for WO and configuration snapshot file management by the 5620 SAM:

- The unit type for the *importSyncInterval* and *workingSyncInterval* parameters is minutes.
- The 5620 SAM raises a critical disk space issue alarm when the amount of disk space is below the value specified by the corresponding *RaiseAlarmWhenSizeLeftInPartitionMb* parameter.
- The 5620 SAM triggers a file purge when the disk space used by the files in an activation subdirectory is greater than the corresponding *MaxSizeInMb* parameter.
- During a file purge, the 5620 SAM sorts the files by age and deletes files according to the file age. The corresponding *PercentToKeepAfterPurge* parameter specifies the percentage of the files that are kept after a purge.
- The 5620 SAM automatically deletes all WO (.xwo) and configuration snapshot (.xcm) files that are older than the number of days specified by the corresponding *DaysToKeep* parameter. Other file types are not deleted.



Note — The 5620 SAM cannot delete files from subdirectories of the *wo_import* directory unless the *samadmin* user has read, write, and execute permissions to the subdirectories.

WO import log management

The 5620 SAM keeps log files for scheduled tasks, including WO imports. You can configure a size constraint policy to limit the number of WO import logs that the 5620 SAM retains. Size constraint policies determine the threshold at which a purge will be performed and the number of logs that will be purged. You can use size constraint policies to specify how the 5620 SAM manages logs and records for various packages and classes. See the *5620 SAM User Guide* for more information about size constraint policies.

File management procedures

Perform the following procedures to configure WO and configuration snapshot disk space usage on the 5620 SAM main server. See the *5620 SAM Parameter Guide* for information about the size constraint parameters in these procedures.

Procedure 6-8 To configure WO and configuration snapshot file management on the 5620 SAM main server

Perform this procedure to configure the disk usage thresholds and file retention settings for WO and configuration snapshot files on the 5620 SAM main server.



Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.



Note 1 — The samadmin user requires read and write permissions to each directory specified in this procedure.

Note 2 — The Solaris command lines in this procedure use the # symbol to represent the command prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

- 1 Log in to the 5620 SAM server station as the samadmin user.
- 2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.
- 3 Create a backup copy of the nms-server.xml file.
- 4 Open the nms-server.xml file using a plain-text editor.
- 5 Search for the following XML tag:

```
<activation
```

- 6 Configure the following fields for WO file management:

- importDaysToKeep="*days*"
- importMaxSizeInMb="*max_size*"
- importPercentToKeepAfterPurge="*percent_to_keep*"

where

days is the amount of time, in days, that the 5620 SAM will keep WO files in the activation/wo_import directory

max_size is the specified maximum amount of disk space, in Mb, that the 5620 SAM allocates for WO files

percent_to_keep is the percentage of files that are retained after a file purge

7 Configure the following fields for configuration snapshot file management:



Note — The maximum value for `snapshotExportsDaysToKeep` is 14 days. If you enter a value higher than 14, configuration snapshot files will still be deleted after 14 days.

- `snapshotExportsDaysToKeep="days"`
- `snapshotExportsMaxSizeInMb="max_size"`
- `snapshotExportsPercentToKeepAfterPurge="percent_to_keep"`

where

`days` is the amount of time, in days, that the 5620 SAM will keep configuration snapshot files in the `activation/snapshot_export` directory

`max_size` is the specified maximum amount of disk space, in Mb, that the 5620 SAM allocates for configuration snapshot files

`percent_to_keep` is the percentage of files that are retained after a file purge

- 8 Save and close the `nms-server.xml` file.
- 9 Navigate to the 5620 SAM server binary directory, typically `/opt/5620sam/server/nms/bin`.
- 10 Enter the following command at the prompt:

```
# ./nmsserver.bash read_config ↵
```

The 5620 SAM main server reads the `nms-server.xml` file and puts the configuration change into effect.

- 11 Close the console window.
-

Procedure 6-9 To delete a WO from the 5620 SAM server

- 1 Choose Manage→Mobile Access→Activation from the 5620 SAM main menu. The Activation form opens.
 - 2 Choose Work Order (Activation) from the object drop-down list.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of WOs is displayed.
 - 4 Select a WO from the list and click on the Delete button. A dialog box appears.
 - 5 Click on the Yes button. The WO is deleted.
 - 6 Close the Activation form.
-

Procedure 6-10 To view WO import logs

WO import logs display errors and warning information for specific WO files.

- 1 Choose Manage→Mobile Access→Activation from the 5620 SAM main menu. The Activation form opens.
 - 2 Choose Import Log (Activation) from the object drop-down list.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of WO import logs is displayed.
 - 4 Select a WO import log from the list and click on the Properties button. The Import Log (View) form opens with the General tab displayed.
 - 5 View the information in the form, as required.
 - 6 Close the Import Log (View) form.
 - 7 Close the Activation form.
-

Procedure 6-11 To delete a WO import log from the 5620 SAM server

- 1 Choose Manage→Mobile Access→Activation from the 5620 SAM main menu. The Activation form opens.
 - 2 Choose Import Log (Activation) from the object drop-down list.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of WO import logs is displayed.
 - 4 Select a WO import log from the list and click on the Delete button. A dialog box appears.
 - 5 Click on the Yes button. The WO import log is deleted.
 - 6 Close the Activation form.
-

Procedure 6-12 To configure the default size constraint policy for WO import logs

- 1 Choose Administration→Size Constraint from the 5620 SAM main menu. The Size Constraint Policies form opens.
- 2 Configure the filter criteria, if required, and click on the Search button. A list of size constraint policies is displayed.

- 3 Select the SAM Default for Work Order Import Logs (Policy ID 5) from the list and click on the Properties button. The Size Constraint Policy (Edit) form opens.



Note — You cannot create a new policy to configure the size constraint parameters for the Work Order Import Logs class. You must modify the default policy.

- 4 Configure the parameters:
 - Threshold (# of objects)
 - Objects To Be Deleted When Threshold Exceeded (# of objects)
 - Apply Threshold To
 - 5 Click on the OK button. A dialog box appears.
 - 6 Click on the Yes button to confirm the action. The Size Constraint Policies form reappears with the default policy displayed in the list with the modified parameters.
 - 7 Close the Size Constraint Policies form.
-

7 — *eNodeB online configuration*

- 7.1 Online configuration overview 7-2**
- 7.2 Workflow to manage online configuration 7-5**
- 7.3 ENB Equipment and eNodeB NE instance objects 7-5**
- 7.4 Logical objects manager 7-10**
- 7.5 9400 NEM support 7-11**

7.1 Online configuration overview

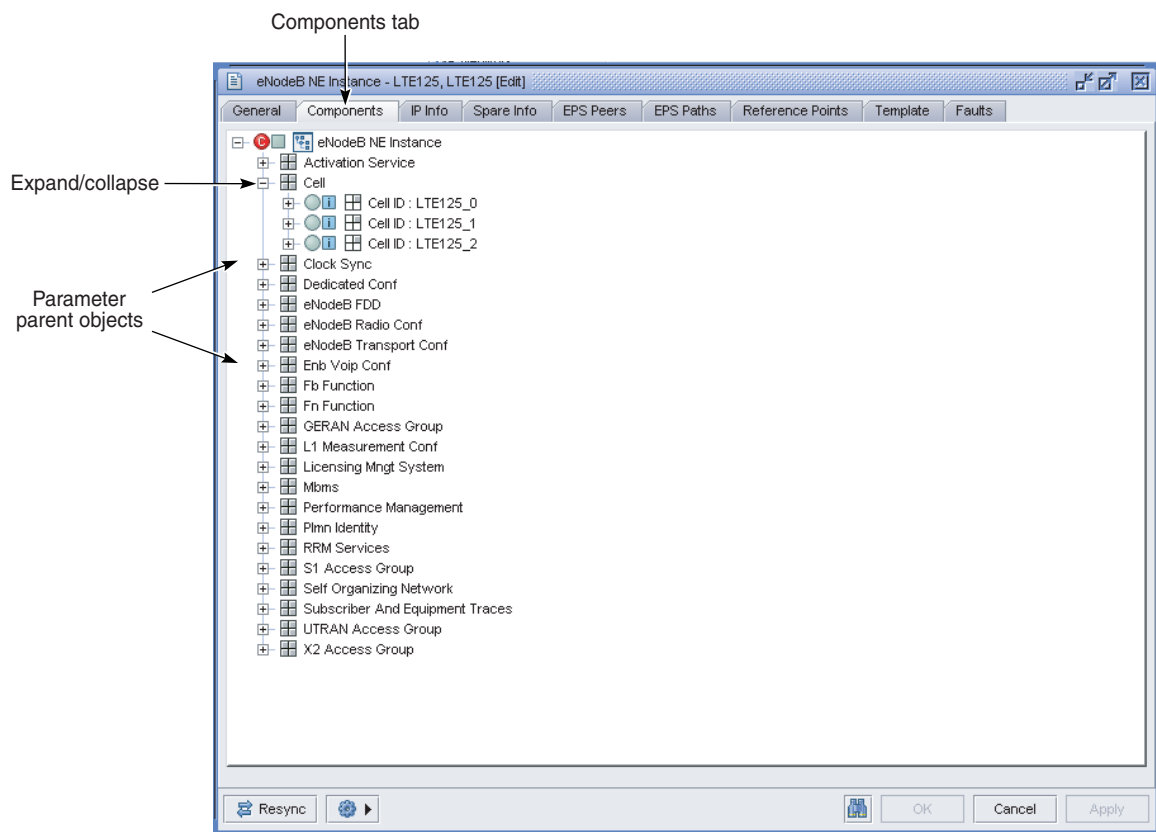
Online configuration is the process of configuring eNodeB parameters using the 5620 SAM GUI, OSS interface, or the 9400 NEM. The information in this chapter is limited to eNodeB managed objects.

Object component tree

You can view the eNodeB object component tree by opening the properties forms for the ENB Equipment object and eNodeB instance and clicking on the Components tab button. See Procedures 7-1 and 7-2 for more information about opening the properties forms for the ENB Equipment and eNodeB NE Instance objects of an eNodeB NE.

See Figure 7-1 for an example of the component tree view of the eNodeB NE Instance and Cell objects.

Figure 7-1 eNodeB NE Instance component tree



22489

You can expand logical parent objects and open the properties forms of child objects using the right-click contextual menu.



Note — Online configuration of the eNodeB does not utilize the engineering and validity checks that are present in WO deployment with the 5620 SAM activation manager (offline configuration). In order to prevent critical inconsistencies in eNodeB configuration, object create and delete actions are not supported for online configuration of eNodeBs.

See chapter 6 for more information about using offline configuration to deploy a WO to one or more eNodeBs.

Object logical view

The logical view provides a simplified interface for accessing eNodeB NE instance child objects for online configuration. You use the logical view to access the properties forms of the following objects:

- cells
 - LTE neighboring cell relations
 - LTE neighboring frequency configurations
- S1-MME reference points
- sectors
- X2 reference points

See Procedure 7-3 for more information about using the logical view.

eNodeB parameters

It is important to understand the following information before configuring eNodeB parameters using online configuration in the 5620 SAM.

eNodeB parameter visibility

The eNodeB parameters are categorized by access into the following visibility levels:

- Customer—Read and write access is available to customers.
- Manufacturer—Read and write access is not available to customers. These parameters are set in the factory or at commissioning.

eNodeB parameter categories

eNodeB parameters are categorized as alpha, beta, gamma, and inventory.

Alpha parameters are transport-related parameters that are required for OAM communication between the eNodeB and the 5620 SAM. Alpha parameters are part of the eNodeB SNMP MIB. Default values for some alpha parameters are set in the factory and are configurable during commissioning using the 9400 NEM. Alpha parameters include the following:

- DHCP parameters
- OAM IP address
- OAM VLAN parameters

Beta parameters are eNodeB hardware and site-specific parameters, and are set on site at commissioning. Beta parameters include the following:

- antenna, RF, and sector definition
- BTS location
- clock configuration
- alarm configuration and data
- NTP server IP address

Gamma parameters are the telecommunications parameters of the eNodeB MIM, and are configured by the 5620 SAM. Gamma parameters include the following:

- eNodeB name
- cell definitions
- S1/X2 link definitions
- telecom IP, VLAN, and IPsec information
- QoS
- neighbor lists

Inventory parameters are read-only 3GPP-compliant parameters that are retrieved through SNMP from FRUs during device discovery.

eNodeB parameter classes

The eNodeB gamma parameters are classified by device impact into the following three classes:

- **Class A (high service impact)**—A full reset occurs on the eNodeB when you modify class A parameters, which is service-affecting. The eNodeB OAM interface is unavailable during the device reset. See Figure 7-2 for the class A icon.
- **Class B (moderate service impact)**—A reset or temporary lock of an eNodeB component, cell, or application occurs when you modify class B parameters, which can be service-affecting. The eNodeB OAM interface remains available. See Figure 7-3 for the class B icon.
- **Class C (no service impact)**—A reset does not occur on the eNodeB when you modify class C parameters. No services are affected. Class C parameters do not have an identifying icon.

Figure 7-2 Class A parameter icon



Figure 7-3 Class B parameter icon



Clear parameters

eNodeB parameters can be left unset or cleared. An unset parameter is the equivalent of an absent parameter in the terminology of the eNodeB MIM. A cleared parameter in the eNodeB MIM contains absolutely no value. Integer parameters are set to their default value or a special value (such as -1) when cleared.

RAN license impact

Some eNodeB parameters determine the consumption of RAN license entitlement tokens. Online configuration can be used to configure RAN license-impacting parameters in order to increase or decrease RAN entitlement token consumption. See chapter 9 for more information about RAN licensing. See Appendix B for mapping information between eNodeB parameters and RAN license entitlements, including the parent object hierarchy for each license-impacting parameter.

7.2 Workflow to manage online configuration

- 1 Configure eNodeB device parameters by opening the properties forms parameter parent objects.
 - Open the properties form of the ENB Equipment object. See Procedure 7-1.
 - Open the properties form of the eNodeB NE Instance object. See Procedure 7-2.
- 2 Open the logical view for eNodeB NE instances, as required. See Procedure 7-3.
- 3 Lock and unlock eNodeBs, as required. See Procedure 7-4.
- 4 Use the logical objects manager to access parameter objects directly. See Procedure 7-5.
- 5 Launch a 9400 NEM connection to an eNodeB. See Procedure 7-6.

7.3 ENB Equipment and eNodeB NE instance objects

The ENB Equipment object is the root of the parameter tree in the eNodeB NetConf MIM, and is the parent object to the eNodeB instance object. The eNodeB instance object is the parent to radio parameters. From these two parent objects, parameters are further organized into approximately 150 child objects, depending on eNodeB version. Each child object is further subdivided into a range of configurable parameters.

See the *5620 SAM LTE Parameter Reference* for descriptions of the objects and parameters of the eNodeB NetConf MIM.

ENB Equipment and eNodeB NE instance property forms

The parameters and properties of the eNodeB NetConf MIM can be configured in the ENB Equipment and eNodeB NE instance property forms. These property forms contain a variety of configurable and read-only parameters in the General tab and other tab areas, however, the majority of child objects are accessed in the Components tab. The contents of the Components tab are presented in a hierarchical tree format. Child objects also have their own properties forms and components tabs.

The eNodeB instance is the parent object to several objects that are important for online configuration. The eNodeB NetConf object structure varies between eNodeB software versions. The following list includes some of these objects:

- Activation Service—This object contains parameters for enabling or disabling eNodeB features such as ANR, PCI, and IRAT HO.
- Cell—This object is the parent to LTE cells.
- Self Organizing Network—This object is the parent to SON objects that specify neighbor relations settings between eNodeBs.
- Subscriber and Equipment Traces—This object is the parent to call trace objects and can be used to create call trace sessions.

Deleting the ENB Equipment object

You can delete the ENB Equipment object by clicking on the Delete button in the Network Element form.



Caution — Deleting the ENB Equipment object for an active eNodeB will disable the eNodeB until a complete reconfiguration is performed. This is not a recommended action.

Deleting the ENB Equipment object for an active eNodeB erases the contents of the NetConf MIM and is highly service-affecting, as the eNodeB will require a complete reconfiguration. Some SNMP parameters in the device MIB may also be affected by the delete operation, which may affect communications between the eNodeB and the 5620 SAM.

The only time when you should delete the ENB Equipment object is to reset parameter settings for pre-provisioned NE instances that have not yet been associated with a live eNodeB. For example, you can delete the ENB Equipment object in a situation where the wrong WO was associated with a pre-provisioned NE instance and a complete reconfiguration of the NE template is required.

ENB Equipment and eNodeB NE instance procedures

Perform the following procedures to access the properties forms for the ENB Equipment and eNodeB NE instance objects. See the *5620 SAM LTE Parameter Reference* for more information about the parameters that can be accessed using the following procedures.

Procedure 7-1 To open an ENB Equipment properties form

Perform this procedure to access the ENB Equipment properties form and configure the contained parameters.



Caution — Configuring the parameters contained in the ENB Equipment properties form can cause a full or partial reset, which is service-affecting.

- 1 Choose one of the following:
 - a Use the navigation tree to select an eNodeB:
 - i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
 - ii Expand the view in order to locate an eNodeB.
 - iii Right-click on an eNodeB and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
 - iv Click on the Properties button in the ENB Base Configuration panel. The ENB Equipment (Edit) form opens with the General tab displayed and a dialog box appears.
 - v Click on the Yes or No button to specify whether changes to the ENB Equipment form will be managed by the containing Network Element form.
 - b Use the equipment manager to select an ENB Equipment object directly:
 - i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment list form opens.
 - ii Choose ENB Equipment (LTE) from the object type drop-down list.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of ENB Equipment objects is displayed.
 - iv Select an ENB Equipment object from the list and click on the Properties button. The ENB Equipment (Edit) form opens with the General tab displayed.
 - 2 Configure the parameters, as required.
 - 3 Click on the Apply button in the ENB Equipment (Edit) form and the Network Element (Edit) form, if required, in order to save the configuration changes.
-

Procedure 7-2 To open an eNodeB NE instance properties form

Perform this procedure to access the eNodeB instance form and configure the contained parameters.



Caution — Configuring the parameters contained in the eNodeB instance properties form can cause a full or partial reset, which is service-affecting.

- 1 Choose one of the following:
 - a Use the navigation tree to select an eNodeB.
 - i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
 - ii Expand the view in order to locate an eNodeB.
 - iii Right-click on an eNodeB and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
 - iv Select the eNodeB instance object in the ENB Instances panel and click on the Properties button. The eNodeB NE Instance (Edit) form opens with the General tab displayed.
 - b Use the logical objects manager to select an eNodeB NE instance directly.
 - i Choose Manage→Mobile Access→eNodeB Logical Objects from the 5620 SAM main menu. The Manage eNodeB Logical Objects list form opens.
 - ii Choose eNodeB NE Instance (LTE) from the object type drop-down list.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of eNodeB instances is displayed.
 - iv Select an eNodeB instance from the list and click on the Properties button. The eNodeB NE Instance (Edit) form opens with the General tab displayed.
- 2 Configure the parameters in the following tabs, as required:
 - General
 - IP Info
 - Spare Info
- 3 To open the Properties form of a child object of the eNodeB instance:
 - i Click on the Components tab button.
 - ii Expand the tree to display the objects, as required.
 - iii Right-click on an object and choose Properties from the contextual menu. The *object_type* (Edit) form opens with the General tab displayed.

- iv Configure the parameters, as required.
 - v Click on the OK button. The form closes.
 - 4 To save the changes:
 - i Click on the Apply button in the eNodeB NE Instance (Edit) form. A dialog box appears.
 - ii Click on the Yes button. The changes are saved.
 - 5 Close the eNodeB Instance (Edit) form.
-

Procedure 7-3 To open the eNodeB NE instance logical view

- 1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
 - 2 Expand the view in order to locate an eNodeB.
 - 3 Right-click on an eNodeB and choose Logical View from the contextual menu. The Equipment-E-NODEB INSTANCE-*eNodeB_name* window opens.
 - 4 To view objects, expand the component tree.
 - 5 To open the properties form of an object, right-click on the object and choose Properties from the contextual menu.
 - 6 Configure parameters and save the changes, as required.
-

Procedure 7-4 To lock or unlock an eNodeB



Danger — You must ensure that the Current Operational State parameter displays a value of “Disabled” before attempting maintenance of eNodeB hardware by onsite technicians. The Current Operational State is displayed in the States tab of the ENB Equipment properties form. Alcatel-Lucent recommends using the Current Operational State parameter as the indicator of eNodeB transmission status.



Caution 1 — Locking an eNodeB disables radio resources on the NE, which is service-affecting.

Caution 2 — Locking an eNodeB prevents configuration changes.

- 1 Perform Procedure [7-1](#) to open the ENB Equipment properties form for an eNodeB.
- 2 Click on the States tab button.

- 3 Perform one of the following:
 - a To lock the eNodeB, choose Locked from the Administrative State drop-down list.
 - b To unlock the eNodeB, choose Unlocked from the Administrative State drop-down list.
- 4 Click on the Apply button. A dialog box appears.
- 5 Click on the Yes button. The lock or unlock request is sent to the NE.



Danger — An eNodeB may still be transmitting if the Administrative State parameter does not display as “Locked”.



Note — When the lock/unlock request is sent to the eNodeB and a deployment failure occurs, the 5620 SAM raises a deployment failure alarm and the Administrative State parameter displays “Locking in Progress” or “Unlocking in Progress”. The eNodeB transmissions status is unaffected by user action at this time.

- 6 Verify that the displayed value of the Administrative State parameter is “Locked” or “Unlocked”.
 - 7 Verify that the Current Operational State parameter displays the expected transmission status (“Enabled” or “Disabled”).
 - 8 Close the ENB Equipment form.
-

7.4 Logical objects manager

The eNodeB logical objects manager allows operators to access the Properties forms of multiple objects simultaneously. You can use the logical objects manager to modify service-affecting settings across multiple devices to synchronize eNodeB resets that result from class A or B parameter modifications and minimize network impact. You can also use the logical objects manager to browse dynamic managed objects such as X2 connections between eNodeBs.

Logical objects manager procedures

Perform the following procedures to access and modify objects using the logical objects manager. See the *5620 SAM LTE Parameter Reference* for more information about the objects and parameters that can be configured using the logical objects manager.

Procedure 7-5 To access and modify objects with the logical objects manager

Perform this procedure to access the Properties form of multiple objects simultaneously.



Caution — When you modify class A and B parameters, a full or partial reset of their parent eNodeB will occur, which is service-affecting.

- 1 Choose Manage→Mobile Access→eNodeB Logical Objects from the 5620 SAM main menu. The Manage eNodeB Logical Objects list form opens.
- 2 Select an object type from the Select Object Type drop-down menu.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of objects is displayed.
- 4 Choose multiple objects by pressing and holding the CTRL key and clicking on an object.
- 5 Click on the Properties button to display the properties form for the selected objects. A single Properties form opens with *(Multiple Instances)* specified.



Note — Navigating to a child object form from a multiple instance Properties form, such as from a multiple instance eNodeB NE Instance form to the Cell form, will open a single instance of the child form and is not a recommended action. Use the logical objects manager to directly open multiple instances of child objects.

- 6 Configure the parameters contained in the multiple instance Properties form, as required, and save the changes.

7.5 9400 NEM support

The 5620 SAM supports the launching of up to two simultaneous 9400 NEM sessions from a single 5620 SAM client application. You can use the 9400 NEM launch function to connect to an eNodeB that is located in a different subnet than the 5620 SAM client application. The 9400 NEM connection will persist in the case of a restart of the 5620 SAM main server.

The following restrictions apply to 9400 NEM support with the 5620 SAM:

- Only one 9400 NEM session can be used to connect to a single eNodeB from the 5620 SAM client application at one time.
- The 9400 NEM session must be closed if the IP address of the eNodeB changes or if the eNodeB changes to an unmanaged state.

- The use of two simultaneous 9400 NEM sessions on a single 5620 SAM client application may result in system instability. Alcatel-Lucent recommends limiting 9400 NEM usage to a single session per client application.
- The 9400 NEM connection to the eNodeB is lost when the 5620 SAM main server performs an activity switch to the redundant server.

See the *Alcatel-Lucent 9400 eNodeB Network Element Manager (NEM) User Guide 418-000-390* for more information about using the 9400 NEM.

9400 NEM launch procedures

Perform the following procedures to launch the 9400 NEM from the 5620 SAM client GUI.

Procedure 7-6 To launch the 9400 NEM from the 5620 SAM client GUI

Perform this procedure to launch a 9400 NEM instance and connect directly to an eNodeB. You must have a 5620 SAM user account with an administrator or eNodeB NEM operator scope of command role in order to launch the 9400 NEM from the 5620 SAM client GUI.

- 1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
- 2 Expand the tree view and locate the appropriate eNodeB.
- 3 Right-click on an eNodeB and choose Launch NEM from the contextual menu. The 9400 NEM launches and attempts to connect to the eNodeB.



Note — You can also launch the 9400 NEM from the Network Element form of an eNodeB by clicking on the More Actions button and choosing Launch NEM.

LTE RAN management

- 8 – LTE RAN device management
- 9 – LTE RAN licensing
- 10 – LTE RAN EPS path management
- 11 – LTE RAN security
- 12 – LTE RAN SON management

8 — *LTE RAN device management*

- 8.1 Overview 8-2**
- 8.2 Workflow for LTE RAN management 8-2**
- 8.3 eNodeB support 8-2**
- 8.4 Inventory management 8-3**
- 8.5 Object life cycle management 8-4**
- 8.6 Bulk operations 8-4**
- 8.7 eNodeB SSH sessions 8-5**
- 8.8 IPv4 address migration 8-5**
- 8.9 IPv6 provisioning and migration 8-9**
- 8.10 Rehomings of eNodeBs between 5620 SAM servers 8-12**

8.1 Overview

This chapter contains information about the following:

- 5620 SAM support of the eNodeB
- the applicability of general 5620 SAM functions in regards to eNodeB management
- IP migration tasks
- rehomining tasks

8.2 Workflow for LTE RAN management

- 1 Review eNodeB support information. See section [8.3](#) for more information.
- 2 Generate inventory lists for eNodeB cards. See Procedure [8-1](#) for more information.
- 3 Manage eNodeB object life-cycle. See section [8.5](#) for more information.
- 4 Manage eNodeB IPv4 to IPv4 address migration. See section [8.8](#) for more information.
- 5 Manage eNodeB IPv4 to IPv6 address migration. See section [8.9](#) for more information.
- 6 Manage eNodeB rehomining between 5620 SAM servers. See section [8.10](#).

8.3 eNodeB support

Table [8-1](#) lists the eNodeB releases supported by the 5620 SAM.

Table 8-1 Supported eNodeB releases

eNodeB release	Technology
eNodeB LA2.0	FDD
eNodeB TLA2.1	TDD
eNodeB LA3.0	FDD
eNodeB TLA3.0	TDD
eNodeB LA4.0	FDD
eNodeB TLA4.0	TDD

The 5620 SAM displays the following physical components in the equipment tree:

- eNodeB (NE)
- D2U (shelf level)
- CB (eCCM with GigEMDA)
- BB (eCEM)
- RRH
- antenna port
- TRDU
- FRU

8.4 Inventory management

This section provides general steps for managing eNodeB equipment inventory. See the *5620 SAM User Guide* for information about general inventory management.

Inventory procedures

Perform the procedures in this section to manage eNodeB control board and base band card inventory.

Procedure 8-1 To inventory eNodeB control board and base band cards

- 1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.
- 2 Choose Card→IO Card→Base Card (Physical Equipment) from the object type drop-down list.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of cards is displayed.



Note — An unfiltered search displays a list of both base band and control board cards. You can specify column filters in order to display a single card type.

- 4 Perform the following tasks, as required.
 - a Remove columns:
 - i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display form opens.
 - ii In the Displayed on Table list box, choose the columns that you need to remove from the table and click the left arrow. The specified columns are moved to the Available for Table list box.
 - iii Click on the OK button. The changes are applied, the Column Display form closes, and the specified columns are removed from the table.
 - b Save the inventory output in HTML or CSV format:
 - i Right-click on a column heading of the inventory output and choose Save to File from the contextual menu. The Save form opens.
 - ii Specify the location to save the file by configuring the Save In parameter.
 - iii Specify the file name by configuring the File Name parameter.
 - iv Configure the Files of Type parameter to choose HTML or CSV format for the inventory output.
 - v Click on the Save button. The results of the inventory search are saved to the specified file.
 - 5 Close the form.
-

8.5 Object life cycle management

You can set the OLC State parameter of network objects to Maintenance or In-Service in order to filter alarms in the Alarms Window. Alarms are generated for network objects regardless of the OLC state. The OLC State parameter is not deployed to devices or services. See the *5620 SAM User Guide* for more information about managing object OLC states.

8.6 Bulk operations

The 5620 SAM does not currently support the use of the bulk operations function to modify eNodeB parameters and objects. Use the logical objects manager to configure multiple instances of a managed object type simultaneously. See section 7.4 for more information about using the logical objects manager.

8.7 eNodeB SSH sessions

The launching of SSH sessions to eNodeBs from the 5620 SAM GUI is intended for use by Alcatel-Lucent support personnel only. Alcatel-Lucent does not recommend using SSH sessions for customer configuration or troubleshooting of the eNodeB.

8.8 IPv4 address migration

This section describes the procedure for migrating 5620 SAM management of the eNodeB from the current management IPv4 address (the source address) to a new management IPv4 address (the target address). You must complete the following tasks in order to successfully complete IPv4 migration:

- 1 add the target IP addresses or ranges to the discovery rule that is currently in use for IPv4 eNodeB management
- 2 configure the relevant IPv4 address parameters on the VLAN:0→Traffic Descriptor→Traffic Descriptor ID: 0 object using offline or online configuration
- 3 wait for the eNodeBs to restart
- 4 re-scan the discovery rule
- 5 confirm that the following conditions are true for each eNodeB:
 - the Active Management IP parameter is updated
 - a full resynchronization has occurred
 - PM statistics data is being collected, if applicable
 - call trace data is being collected, if applicable

You must add the target IPv4 addresses to the the discovery rule that contains the source IPv4 addresses. Creating a new discovery rule for the target IPv4 addresses causes the 5620 SAM to continue using the source IPv4 addresses and results in the loss of OAM communication. If a new discovery rule must be created for the target IPv4 addresses, then the affected eNodeBs must be deleted from the managed network before 5620 SAM discovery of the target IPv4 addresses is attempted. Due to the loss of management data that results from this operation, this course of action is not recommended.

See the *5620 SAM Parameter Guide* for more information about the parameters that are described in the following procedure. See the *5620 SAM LTE Parameter Reference* for more information about eNodeB VLAN parameters.

Procedure 8-2 To migrate 5620 SAM management of eNodeBs between IPv4 addresses



Warning — Performing this procedure causes a full reset of the affected eNodeBs, which is service-affecting.



Note 1 — This procedure is supported for eNodeB release LA3.0 and later.

Note 2 — This procedure must be completed within a 30 min time frame. The eNodeBs will automatically revert back to the source IPv4 address if 5620 SAM management via the target IP addresses is not achieved within 30 mins of performing step 2.

This procedure assumes that the following conditions are true:

- one or more discovery rules for IPv4 management of eNodeBs exist in the 5620 SAM network
 - eNodeBs are discovered and managed over IPv4 using an IPv4-based discovery rule
 - eNodeB management IPv4 addresses are reachable from the 5620 SAM main server
 - call trace and PM statistics data is being collected, if enabled
- 1 Add the target IPv4 address rule elements to the discovery rule that is currently being used to manage the eNodeBs.



Warning — You must add the target IPv4 addresses or ranges to the existing IPv4-based discovery rule or rules for eNodeB management. Creating a new discovery rule for the target IPv4 addresses causes the 5620 SAM to continue using the source IPv4 addresses and results in the loss of OAM communication.

- i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the General tab displayed.
- ii Configure the filter criteria, if required, and click on the Search button. A list of discovery rules is displayed.
- iii Select the appropriate discovery rule from the list and click on the Properties button. The Topology Discovery Rule (Edit) form opens with the General tab displayed.
- iv Click on the Rule Elements tab button.
- v Click on the Create button. The Topology Discovery Rule Element (Create) form opens.
- vi Configure the parameters:
 - IP Address
 - Mask Bits
 - Usage



Note — Alcatel-Lucent recommends using IPv4 address ranges to discover eNodeBs.

- vii Click on the OK button. The form closes and the rule element is added to the discovery rule.
 - viii Repeat sub steps v to vii in order to create additional rule elements, as required.
 - ix Click on the OK button in the Topology Discovery Rule (Edit) form. The form closes.
 - x Click on the Apply button in the Discovery Manager (Edit) form. A dialog box appears.
 - xi Click on the Yes button. The changes to the discovery rule are saved.
- 2 Choose one of the following:
- a Configure the management IPv4 address of the eNodeBs using offline configuration.
 - i Create a WO for IPv4 migration using the 9952 WPS. See the *9952 WPS User Guide* for more information.
 - ii Transfer the WO file from the 9952 WPS server to the 5620 SAM main server. See the *9952 WPS User Guide* for more information.
 - iii Create an activation session. See Procedure 6-1 for more information.
 - iv Deploy the WO using the activation manager. See Procedure 6-2 for more information.
 - b Configure the management IP of the eNodeBs using online configuration.
 - i Open the properties form of the eNodeB NE instance. See Procedure 7-2 for more information.
 - ii Click on the Components tab button.
 - iii Expand the component tree to view the *Traffic Descriptor ID: 0* object. The path is eNodeB NE Instance→eNodeB Transport Conf→eNodeB Transport Conf ID: 0→VLAN→VLAN ID: 0→Traffic Descriptor→ Traffic Descriptor ID: 0.
 - iv Right-click on the *Traffic Descriptor ID: 0* object and choose Properties from the contextual menu. The Traffic Descriptor - 0 (Edit) form opens with the General tab displayed.
 - v Configure the parameters in the IPv4 panel:
 - ipv4Address
 - ipv4AddressFirstHopRouter
 - ipv4SubNetMask
 - vi Click on the OK button. The Traffic Descriptor - 0 (Edit) form closes.
 - vii Click on the Apply button in the eNodeB NE Instance (Edit) form. A dialog box appears.

- viii Click on the Yes button. The changes are saved and a full reset of the eNodeB is initiated.
 - ix Repeat sub steps i to viii for the remaining eNodeBs, as required.
- 3 Wait for the affected eNodeBs to reset. The 5620 SAM raises major ReachabilityProblem alarms against the eNodeBs that are undergoing IP migration.
- 4 Re-scan the discovery rule until the 5620 SAM discovers the eNodeBs using the target IPv4 address.



Note 1 — The 5620 SAM clears the ReachabilityProblem alarm and raises a NodeRebooted alarm when the eNodeBs are discovered and managed using the target IPv4 address.

Note 2 — The reboot and discovery process can take up to 10 minutes to complete.

Note 3 — If you have created a new discovery rule, you must turn down the previous discovery rule and delete the eNodeBs from the managed network before using the new discovery rule to scan the target IPv4 address ranges. See Procedure 5-12 for more information about unmanaging and deleting eNodeBs.

- i Choose Administration→Discovery Manager from the 5620 SAM main menu, if required. The Discovery Manager (Edit) form opens with the General tab displayed.
 - ii Click on the Discovery Rules tab button, if required.
 - iii Click on the Rescan button. A dialog box appears.
 - iv Click on the Yes button. The 5620 SAM re-scans the IPv4 address rule elements that are specified in the discovery rule.
 - v Repeat sub steps iii and iv, as required.
- 5 Verify that the active management IP addresses of the eNodeBs have been updated.
 - i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment list form opens.
 - ii Choose Network Element (Network) from the object type drop-down list.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of NEs is displayed.
 - iv Select an eNodeB from the list and click on the Properties button. The Network Element (Edit) form opens with the General tab displayed.
 - v Verify the value of the Active Management IP parameter against the corresponding target IPv4 address for the eNodeB.
 - vi Repeat sub steps iv and v, as required.

- 6 Verify that the eNodeBs are fully resynchronized.
 - i Choose Administration→Discovery Manager from the 5620 SAM main menu, if required. The Discovery Manager (Edit) form opens with the General tab displayed.
 - ii Click on Resync Status tab button.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of NEs is displayed.
 - iv Verify the status of the full resynchronization by viewing the data displayed in the Resync Status column.
 - 7 Verify that PM statistics files are being saved to the `/opt/5620sam/lte/stats/<date>/eNodeB` directory on the target 5620 SAM server.
 - 8 Verify that call trace files are being saved to the `/opt/5620sam/calltrace` and `/opt/5620sam/debugtrace` directories on the target auxiliary 5620 SAM server.
-

8.9 IPv6 provisioning and migration

You can use the 5620 SAM to configure the eNodeB for OAM and telecom traffic over IPv6. Before you can enable IPv6 OAM management on an eNodeB, you must perform the following tasks:

- Plumb and enable an IPv6 interface on each 5620 SAM main server station. See the appropriate OS documentation for information about configuring IPv6 interfaces.
- Configure the 5620 SAM to manage devices using IPv6 in the server installer. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information about enabling IPv6 support using the 5620 SAM installer. A reinstallation of the 5620 SAM is not required.

IPv6 migration procedure

The procedure in this section describes the general tasks for migrating 5620 SAM management of eNodeBs from IPv4 to IPv6. The information in this section applies to eNodeBs that are managed by the 5620 SAM over IPv4 and must be migrated to IPv6 management. See the *5620 SAM Parameter Guide* for more information about the parameters that are described in the following procedure.

See the *Alcatel-Lucent 9400 | Release LAx.x-TLx.x Migration to IPv6 (Telecom and OAM) Procedure 418-000-052* for more information about IPv6 migration.

Procedure 8-3 To migrate 5620 SAM management of eNodeBs from IPv4 to IPv6

This procedure describes the general steps for IP migration that require the 5620 SAM. This procedure does not describe preparation steps, such as importing parameter templates, or steps that are performed using the 9952 WPS.



Warning 1 — Performing this procedure causes a full reset of the affected eNodeBs, which is service-affecting.

Warning 2 — Performing this procedure requires the unmanaging and deleting of eNodeBs, which results in the loss of management data.



Note 1 — IPv6 management is supported on eNodeB release LA3.0 and later.

Note 2 — This procedure must be completed within a 30 min time frame. The eNodeB will automatically revert back to IPv4 format if IPv6 OAM management is not achieved within 30 mins of performing step 2.

This procedure assumes that the following conditions are true:

- one or more discovery rules for IPv4 management of eNodeBs exist in the 5620 SAM network
 - eNodeBs are discovered and managed over IPv4 using the IPv4 discovery rules
 - eNodeB management IPv4 addresses are reachable from the 5620 SAM main server
 - call trace and PM statistics data is being collected, if enabled
- 1 Create one or more discovery rules for eNodeB management and specify IPv6 for the Management Protocol parameter. See Procedure 5-6 for more information.
 - 2 Choose one of the following:



Note 1 — Step 2 a is intended for multiple eNodeBs. Step 2 b is intended for a single eNodeB, but not for multiple NEs.

Note 2 — The IP parameters of the VLAN: 1 object (telecom traffic) must be set before or simultaneously as the VLAN: 0 object (OAM traffic). If the VLAN: 1 object is not configured for IPv6, then configure the IP parameters of the VLAN: 1 object for IPv6 at the same time as the VLAN: 0 object.

- a Configure the eNodeB device parameters for IP migration using offline configuration.
 - i Create a snapshot instance that includes the eNodeBs that are intended for IP migration. See Procedure 6-4 for more information.
 - ii Take a configuration snapshot in order to capture the current eNodeB parameter configuration. See Procedure 6-5 for more information.
 - iii Transfer the configuration snapshot to the 9952 WPS server. See the *9952 WPS User Guide* for more information.

- iv Create a WO that modifies the required eNodeB parameters for IP migration. See the *Alcatel-Lucent 9400 | Release LAx.x-TLAX.x Migration to IPv6 (Telecom and OAM) Procedure 418-000-052* for more information.
 - v Transfer the WO file from the 9952 WPS server to the 5620 SAM main server. See the *9952 WPS User Guide* for more information.
 - vi Create an activation session. See Procedure 6-1 for more information.
 - vii Deploy the WO using the activation manager. See Procedure 6-2 for more information.
- b Configure the eNodeB device parameters for IP migration using online configuration.
- i Open the properties form of the eNodeB NE instance. See Procedure 7-2 for more information.
 - ii Navigate to the parameter objects and configure the parameters as required for IP migration. See the *Alcatel-Lucent 9400 | Release LAx.x-TLAX.x Migration to IPv6 (Telecom and OAM) Procedure 418-000-052* for more information.
 - iii Save the changes by clicking on the Apply button in the eNodeB NE Instance properties form. A dialog box appears.
 - iv Click on the Yes button. The changes are saved and the NE resets.
- 3 Wait for the eNodeBs to reset. The 5620 SAM raises major ReachabilityProblem alarms against the eNodeBs that are undergoing IP migration. The following conditions must be true when the reset is complete:
- a ping of the eNodeB management IPv4 addresses from the 5620 SAM main server fails
 - a ping of the eNodeB management IPv6 addresses from the 5620 SAM main server succeeds
- 4 Unmanage and delete the eNodeBs from the 5620 SAM network. See Procedure 5-12 for more information.
- 5 Rescan the IPv6 discovery rules by performing the following steps:



Note — If you do not perform this step within 30 mins of performing step 2, then the eNodeBs will automatically fall back to IPv4.

- i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.
- ii Select an IPv6 discovery rule from the list and click on the Rescan button. A dialog box appears.
- iii Click on the Yes button. The 5620 SAM scans the network as specified by the discovery rule.

- iv Click on the Managed State tab button.
 - v Configure the filter criteria, if required, and click on the Search button. A list of managed NEs is displayed.
 - vi Verify that the eNodeBs are managed by the 5620 SAM and successfully resynchronized. The discovery and resync process may take several minutes.
- 6 Verify that all eNodeBs that have been migrated to IPv6 are successfully managed by the 5620 SAM.
 - 7 Create an eNodeB performance management policy and activate PM statistics collection by performing Procedure [14-1](#).
 - 8 Activate call trace sessions for eNodeBs by performing Procedure [15-16](#).
 - 9 Verify that PM statistics files are being saved to the `/opt/5620sam/lte/stats/<date>/eNodeB` directory on the target 5620 SAM server.
 - 10 Verify that call trace files are being saved to the `/opt/5620sam/calldata` and `/opt/5620sam/debugtrace` directories on the target auxiliary 5620 SAM server.
-

8.10 Rehoming of eNodeBs between 5620 SAM servers

This section describes the general procedure for rehoming an eNodeB cluster from one 5620 SAM server (the source server) to another 5620 SAM server (the target server). The procedures described in this section apply to standalone or redundant installations of the 5620 SAM in collocated or distributed configuration.



Note — The procedures in this section are supported for two 5620 SAM servers (source and target) that are both running 5620 SAM Release 9.0 R5.

This section uses the following naming conventions:

- 5620 SAM source server—the 5620 SAM server installation that the eNodeBs are migrated from
- 5620 SAM target server—the 5620 SAM server installation that the eNodeBs are migrated to
- target eNodeBs—the eNodeBs, in a managed state on the 5620 SAM source server, that are to be migrated
- rehomed eNodeBs—the eNodeBs, in a managed state on the 5620 SAM target server, that have been migrated to the 5620 SAM target server

Network configuration details

The procedure described in this section is applicable to the following network configuration:

- 5620 SAM source server—one 5620 SAM server that is connected to one auxiliary (preferred/reserved) server
- 5620 SAM target server—one 5620 SAM server that is connected to one auxiliary (preferred/reserved) server
- two 5620 SAM client applications (source/target)

Workflow for eNodeB rehomings

The following workflow describes the high-level steps that are required in order to rehome eNodeBs between 5620 SAM servers.

- 1 Prepare the main 5620 SAM source server. See Procedure [8-4](#).
- 2 Prepare the main 5620 SAM target server. See Procedure [8-5](#).
 - verify that the required modules are installed
 - verify the call trace auxiliary server configuration
 - configure an NE user and mediation security policy
- 3 Prepare the eNodeBs for rehomings. See Procedure [8-6](#).
 - disable PM statistics collection on the source server
 - disable call trace collection on the source server
 - take a configuration snapshot of the target eNodeBs
 - close all external client sessions
 - unmanage the target eNodeBs
- 4 Discover and manage the rehomed eNodeBs on the target 5620 SAM server. See Procedure [8-7](#).
 - create an equipment group for the rehomed eNodeBs
 - configure a discovery rule
 - verify that the rehomed eNodeBs are successfully managed by the target server
 - activate call trace sessions for the rehomed eNodeBs
 - verify the operational state of the rehomed eNodeBs
 - verify PM statistics collection and call trace for the rehomed eNodeBs
- 5 Delete eNodeB objects on the source 5620 SAM server. See Procedure [8-8](#).
 - delete discovery rule elements
 - delete the unmanaged eNodeBs, if required
- 6 Reverse the rehomings operation, if required. See Procedure [8-9](#).
 - unmanage the rehomed eNodeBs on the target server
 - remanage the rehomed eNodeBs with the source server

Rehomining procedures

Perform the following procedures in sequence in order to rehome the target eNodeBs. Access to the admin account for the 5620 SAM source and target servers is required for the procedures in this section.



Note — The procedures in this section do not describe specific steps for the following tasks:

- migration of PM statistics files
- migration of call trace files
- migration of the alarms database
- navigation of the 9952 WPS client GUI
- data source declaration for the 9959 NPO

Procedure 8-4 To prepare the main 5620 SAM source server

This procedure describes the steps for verifying that the target eNodeBs are managed by the main 5620 SAM source server.

- 1 Log in to the main 5620 SAM source server as the admin user using the client application.
 - 2 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the General tab displayed.
 - 3 Click on the Managed State tab button.
 - 4 Configure the filter criteria, if required, and click on the Search button. A list of managed NEs is displayed.
 - 5 Verify that the target eNodeBs displayed Managed in the Site State column.
 - 6 Close the Discovery Manager (Edit) form.
-

Procedure 8-5 To prepare the main 5620 SAM target server

This procedure describes the steps for verifying that the 5620 SAM target server is configured with the modules, auxiliary servers, RAN license capacity, and mediation objects that are required to manage the rehomed eNodeBs.

- 1 Verify that the required 5620 SAM modules are installed on the target server.
 - i Log in to the main 5620 SAM target server as the admin user using the client application.
 - ii Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens with the General tab displayed.
 - iii Expand the 5620 SAM Modules and Packages Licensed panel, if required.

- iv Verify that the following packages are installed:
 - 5620 SAM Element Manager (SAM-E)
 - 5620 SAM Provisioning (SAM-P)
 - 5620 SAM Assurance (SAM-A)
 - v Close the 5620 SAM License (Edit) form.
- 2 Verify the call trace auxiliary server configuration.
- i Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.
 - ii Click on the Auxiliary Servers tab button.
 - iii Click on the Search button. A list of auxiliary servers is displayed.
 - iv Verify the information that is displayed in the columns.
 - v If required, configure the auxiliary servers with the correct IP addresses, service name, and host name. See the *5620 SAM User Guide* for more information about 5620 SAM system redundancy.
 - vi Close the System Information form.
- 3 Verify the RAN license capacity by performing Procedure 9-3 and verifying that the following conditions are true:
- the License File Import Status parameter displays “succeeded”
 - there is sufficient entitlement capacity to permit the activation of the rehomed eNodeBs
- 4 Configure an NE user and mediation security policy by performing Procedure 5-5.
-

Procedure 8-6 To prepare eNodeBs for rehomings

This procedure describes the steps for disabling PM statistics collection, call trace sessions, and for unmanaging the target eNodeBs on the source 5620 SAM server.

- 1 Disable PM statistics collection by setting the Administrative State of the RAN performance management policy or policies.
- i Choose Tools→Statistics→RAN Performance Management Policies from the 5620 SAM main menu. The RAN Performance Management Policies form opens.
 - ii Configure the filter criteria, if required, and click on the Search button. A list of RAN performance management policies is displayed.
 - iii Select a policy from the list and click on the Properties button. The eNodeB Performance Management Policy (Edit) form opens with the General tab displayed.

- iv Click on the drop-down list for the Administrative State parameter and choose Down. A warning dialog box appears.
- v Click on the OK button. The warning dialog box closes.
- vi Click on the Apply button. A confirmation dialog box appears.
- vii Click on the Yes button. The dialog box and the eNodeB Performance Management Policy (Edit) form close.



Note — You must set the Administrative State to Down for all eNodeB performance management policies that are associated with eNodeBs that are targeted for rehomings.

- 2 Disable call trace collection.
 - i Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions (Edit) form opens with the General tab displayed.
 - ii Click on the Call Trace Sessions tab button.
 - iii Configure the filter for the isTraceActive column in order to display the active call trace sessions.
 - iv Configure the filter for the Site Id column, if required.
 - v Click on the Search button. A list of active call trace sessions is displayed.
 - vi Select one or more active call trace sessions from the list and click on the Deactivate button. A dialog box appears.
 - vii Click on the Yes button. The dialog box closes and the call trace sessions are deactivated.
- 3 Take a configuration snapshot of the target eNodeBs.
 - i Create a snapshot instance that includes the target eNodeBs by performing Procedure [6-4](#).
 - ii Take the configuration snapshot by performing Procedure [6-5](#).
 - iii Transfer the configuration snapshot file to the 9952 WPS server. See the *9952 WPS User Guide* for more information
- 4 Close all client sessions other than the current session.
 - i Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
 - ii Click on the Sessions tab button. A list of active sessions is displayed.
 - iii Select a session from the list and click on the Close Session button. A dialog box appears.
 - iv Click on the Yes button. The session closes.

- v Repeat steps [iii](#) to [iv](#) to close additional sessions, as required.
 - vi Close the 5620 SAM User Security - Security Management (Edit) form.
- 5 Unmanage the target eNodeBs.
- i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the General tab displayed.
 - ii Click on the Managed State tab button.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of managed NEs is displayed.
 - iv Select one or more target eNodeBs from the list and click on the Unmanage button. A dialog box appears.
 - v Click on the Yes button.
 - vi Wait for the state to change to Unmanaged. Supervision of the target eNodeBs is stopped.
 - vii Close the Discovery Manager form.
-

Procedure 8-7 To discover and manage the rehomed eNodeBs on the target 5620 SAM server

This procedure describes the steps for discovering the rehomed eNodeBs on the target 5620 SAM server, verifying successful management, and reactivating PM statistics collection and the call trace function.

- 1 Create an equipment group for the rehomed eNodeBs by performing Procedure [11-1](#), if required.
- 2 Configure a discovery rule and associate the equipment group with the discovery rule by performing Procedure [5-6](#).
- 3 Wait for the discovery process to finish. This may take several minutes.
- 4 Verify that the rehomed eNodeBs are in a managed state by performing Procedure [5-9](#).
- 5 Create an eNodeB performance management policy and activate PM statistics collection by performing Procedure [14-1](#).



Note — You can transfer PM files from the source 5620 SAM server to the target 5620 SAM server. The default location for PM files is /opt/5620sam/lte/stats/<date>/eNodeB/<eNodeB name>. See section [14.3](#) for more information.

- 6 Activate call trace sessions for eNodeBs by performing Procedure [15-16](#).

- 7 Verify the operational state of the rehomed eNodeBs.
 - i Choose Application→Navigation Tree from the 5620 SAM main menu. The Equipment-Network window opens.
 - ii Verify that the rehomed eNodeBs are located in the appropriate equipment group.
 - iii Right-click on an eNodeB and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
 - iv Verify the following in the General tab of the Network Element (Edit) form:
 - the State parameter displays a value of Managed
 - the OLC State parameter displays a value of In Service
 - v Click on the Physical Links tab button.
 - vi Click on the Search button. A list of links is displayed.
 - vii Verify that the links display In Service in the Operational State column.
 - viii Click on the Faults tab button.
 - ix Click on the Search button. If the 5620 SAM has raised alarms against the NE, a list of affecting alarms is displayed.
 - x Resolve fault conditions, if required. See chapter 15 for more information about troubleshooting for eNodeBs. See the *5620 SAM Troubleshooting Guide* for more information about troubleshooting using network alarms. See the *5620 SAM Alarm Reference* for a list of eNodeB alarms.
 - xi Close the Network Element (Edit) form.
 - xii Repeat steps [iii](#) to [xi](#) for additional eNodeBs, as required.
 - 8 Verify that PM statistics files are being saved to the /opt/5620sam/lte/stats/<date>/eNodeB directory on the target 5620 SAM server.
 - 9 Verify that call trace files are being saved to the /opt/5620sam/calltrace and /opt/5620sam/debugtrace directories on the target auxiliary 5620 SAM server.
-

Procedure 8-8 To delete eNodeB objects on the source 5620 SAM server

This procedure describes the steps for deleting the target eNodeBs from the source 5620 SAM server, which removes all NE objects from the managed network.

- 1 Log in to the source 5620 SAM server as the admin user using the client application.
- 2 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the General tab displayed.

- 3 Click on the Managed State tab button.
 - 4 Configure the filter criteria, if required, and click on the Search button. A list of NEs is displayed.
 - 5 Select one or more unmanaged target eNodeBs from the list and click on the Delete button. A dialog box appears.
 - 6 Click on the Yes button. The target eNodeBs are deleted from the source 5620 SAM server.
 - 7 Remove the target eNodeB IP addresses from the source 5620 SAM server discovery policy or policies.
 - i Click on the Discovery Rules tab button.
 - ii Select a discovery rule from the list and click on the Properties button. The Topology Discovery Rule (Edit) form opens with the General tab displayed.
 - iii Click on the Rule Elements tab button.
 - iv Configure the filter criteria, if required, and click on the Search button. A list of rule elements is displayed.
 - v Select one or more rule elements from the list that correspond to the IP addresses or IP ranges of the rehomed eNodeBs.
 - vi Click on the Delete button. The rule elements are deleted.
 - vii Click on the OK button. The Topology Discovery Rule (Edit) form closes.
 - viii Click on the OK button in the Discovery Manager (Edit) form. A dialog box appears.
 - ix Click on the Yes button. The Discovery Manager (Edit) form closes.
-

Procedure 8-9 To reverse the rehomings operation

This procedure describes the fallback steps for reversing the rehomings operation and reverting management of the rehomed eNodeBs from the target 5620 SAM server to the source 5620 SAM server.

- 1 Log in to the target 5620 SAM server as the admin user using the client application.
- 2 Unmanage the rehomed eNodeBs on the target 5620 SAM server.
 - i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the General tab displayed.
 - ii Click on the Managed State tab button.
 - iii Configure the filter criteria, if required, and click on the Search button. A list of managed NEs is displayed.

- iv Select one or more eNodeBs from the list and click on the Unmanage button. A dialog box appears.
 - v Click on the Yes button.
 - vi Wait for the state to change to Unmanaged. Supervision of the eNodeBs is stopped.
 - vii Close the Discovery Manager form.
- 3 Manage the rehomed eNodeBs with the source 5620 SAM server.



Note — You must configure a discovery rule with the required rule elements if you deleted eNodeB objects by performing Procedure 8-8. See Procedure 5-6 for more information about configuring a discovery rule.

- i Log in to the source 5620 SAM server as the admin user using the client application.
 - ii Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the General tab displayed.
 - iii Click on the Managed State tab button.
 - iv Configure the filter criteria, if required, and click on the Search button. A list of NEs is displayed.
 - v Select one or more unmanaged eNodeBs from the list and click on the Manage button. A dialog box appears.
 - vi Click on the Yes button. The 5620 SAM sends a management request to the specified eNodeBs.
 - vii Wait for management to be achieved for each eNodeB.
-

9 — *LTE RAN licensing*

- 9.1 RAN licensing overview 9-2**
- 9.2 Workflow to manage RAN licensing 9-3**
- 9.3 5620 SAM RAN license manager 9-3**
- 9.4 RAN license consumption management 9-7**

9.1 RAN licensing overview

The 5620 SAM supports feature and capacity licensing functions for RAN management through the LKDI online licensing tool and the 5620 SAM RAN license manager. The designated CLM can purchase entitlements using the online LKDI tool and save them as an encrypted license file. The license file can be imported into the 5620 SAM using the RAN license manager.

Feature, capacity, and specific licenses are represented in the network by corresponding entitlements that contain a quantity of purchased tokens. A token represents a single unit of consumable license. RAN license tokens are consumed when features are activated on RAN devices, typically through the Activation Service object. Enumerated license tokens, such as bandwidth, are consumed when RAN device cell parameters are configured to use the corresponding value type. Specific license tokens are consumed when the corresponding parameter objects are configured on RAN devices and cells.

Consider the following information about RAN licensing with the 5620 SAM.

- You must have a user account with a scope of command role that includes the `ranlicense` permission in order to manage RAN licensing. The `ranlicense` permission is included in the Administrator, Network Element Equipment Management, and SAM Management and Operations default scope of command roles.
- Only one license file can be active in the 5620 SAM network at a time.
- You cannot import a license file with a generated date that is older than that of the currently active license file.
- You cannot enable features or add capacity unless there is sufficient number of tokens.
- Tokens can be used, released, and reassigned to other eNodeBs. When you unmanage and/or delete an NE, the all of the tokens that are assigned to the NE are released.
- Temporary licenses have an expiration date, after which time the tokens cannot be distributed to devices.
- Features and capacity are not disabled or removed when active tokens expire. The 5620 SAM raises license alarms on devices that are in a state of license violation.
- A global license violation in the 5620 SAM network will prevent RAN device modifications until the license violation is resolved.
- The expiration of a license entitlement can cause the number of available tokens in the network to become negative. The number of available tokens must be positive before more tokens of that type can be assigned to RAN devices.



Note — You must recompute the RAN license consumption when the 5620 SAM is upgraded from a version that is earlier than Release 9.0 R5. See Procedure [9-5](#) for more information.

See section [9.3](#) for more information about using the RAN license manager. See section [9.4](#) for a listing of RAN license entitlement types and for more information about managing entitlement token consumption. See Appendix [B](#) for information about the mapping between eNodeB parameter objects and RAN license entitlements.

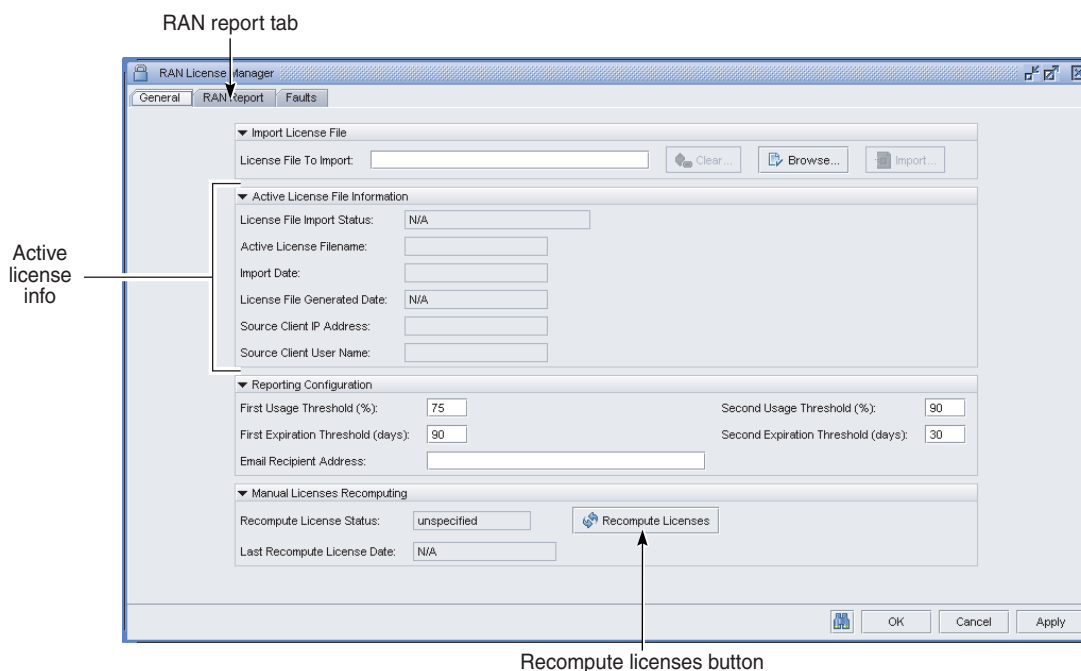
9.2 Workflow to manage RAN licensing

- 1 Acquire RAN license files using the LKDI online licensing tool.
- 2 Import RAN license files to the 5620 SAM using the RAN license manager. See Procedure 9-1.
- 3 Configure notification thresholds for license usage, and specify a recipient e-mail address for license notifications. See Procedure 9-2.
- 4 View RAN license token consumption, as required. See Procedure 9-3.
- 5 Generate RAN license token consumption reports, as required. See Procedure 9-4.
- 6 Recompute RAN license token consumption to resolve license inconsistencies, if required. See Procedure 9-5.
- 7 Manage RAN license token consumption by configuring parameters on RAN devices and cells, as required. See Procedure 9-6.

9.3 5620 SAM RAN license manager

The RAN license manager allows you to view and manage RAN device license allocation in the 5620 SAM network. See Figure 9-1 for a view of the RAN license manager.

Figure 9-1 RAN license manager



22490

You can import an LKDI license file into the 5620 SAM using the RAN license manager. The license file must be in the correct format, contain a valid license signature, and the tokens contained in the license file must correspond to the host ID of the 5620 SAM server. For redundant installations of the 5620 SAM, the license file must contain the host IDs of the active and standby servers. The 5620 SAM continues to use the most recently imported license file when you try to import an invalid license file.

You can configure alarm and notification thresholds for token consumption. Tokens that have reached the specified thresholds display as faulted in the RAN license manager. The 5620 SAM validates a license file during the import operation and raises license violation alarms as required. You can configure the 5620 SAM to send an e-mail notification to a specified address when usage thresholds are crossed.

The RAN license manager displays the active license file in the Active License File Information panel in the General tab of the RAN License Manager form. The Active License File Information panel provides the following information about the active license file:

- license file import status
- file name
- import date
- license file generation date
- IP address of the 5620 SAM client that performed the import operation
- username of the user that performed the import operation

The RAN Report tab of the RAN License Manager form displays the following information about the features, capacities, and tokens of the active license file:

- license name
- license type (capacity, feature, or specific)
- technology type (LTE or W-CDMA)
- total purchased
- total consumed
- total available
- percentage remaining
- expiration date
- days remaining before expiration

RAN license manager procedures

Perform the following procedures to manage RAN license capacity using the RAN license manager. See the *5620 SAM Parameter Guide* for more information about the parameters that are described in the following procedures.

Procedure 9-1 To import a RAN license file using the RAN license manager

You must have a license file from the LKDI on your client computer before you can import the license file into the 5620 SAM.

- 1 Choose Administration→RAN License Manager from the 5620 SAM main menu. The RAN License Manager form opens with the General tab displayed.
 - 2 Review the license file information in the Active License File Information panel, if required.
 - 3 Click on the Browse button in the Import License File panel. The Select RAN License file form opens.
 - 4 Navigate to the location of the license file.
 - 5 Choose the license file and click on the Open button. The license file name displays in the License File To Import field.
 - 6 Perform one of the following steps.
 - a Import the license file.
 - i Click on the Import button. A dialog box appears.
 - ii Select the check box to acknowledge the warning and click on the Yes button to close the dialog. The licenses contained in the license file are imported into the 5620 SAM and the RAN license capacity is updated.
 - b Clear the license file and select another file.
 - i Click on the Clear button. The License File to Import field is cleared.
 - ii Go to step 3 and select another file.
 - 7 Click on the RAN Report tab button.
 - 8 Verify the new license capacity as required.
 - 9 Close the RAN License Manager form.
-

Procedure 9-2 To configure RAN license file reporting

- 1 Choose Administration→RAN License Manager from the 5620 SAM main menu. The RAN License Manager form opens with the General tab displayed.
- 2 Configure the parameters:
 - First Usage Threshold (%)
 - Second Usage Threshold (%)
 - First Expiration Threshold (days)
 - Second Expiration Threshold (days)
 - Email Recipient Address

- 3 Click on the Apply button. A dialog box appears.
 - 4 Click on the Yes button to close the dialog.
 - 5 Click on the Faults tab button.
 - 6 Review any license alarms that result from changes to the threshold parameters, as required.
 - 7 Close the RAN License Manager form.
-

Procedure 9-3 To view the current RAN license file information

- 1 Choose Administration→RAN License Manager from the 5620 SAM main menu. The RAN License Manager form opens with the General tab displayed.
- 2 Review the license file information in the Active License File Information panel.
- 3 Click on the RAN Report tab button.
- 4 Click on the Search button. A list of RAN license entitlements with available and consumed tokens is displayed.



Note — The RAN license information in the RAN Report tab is not automatically refreshed when changes to the token consumption occur while the RAN License Manager form is open. You must click on the Search button to refresh the list.

- 5 Review the information in the list.
 - 6 Close the RAN License Manager form.
-

Procedure 9-4 To generate a RAN license report

You can generate a report file that contains the information displayed in the RAN Report tab of the RAN License Manager form. You can choose HTML or CSV as the format for the generated file.

- 1 Choose Administration→RAN License Manager from the 5620 SAM main menu. The RAN License Manager form opens with the General tab displayed.
- 2 Click on the RAN Report tab button.
- 3 Click on the Generate Report button. The Save As form opens.
- 4 Navigate to the directory that you want to save the report file in.
- 5 Enter a name for the file in the File Name field.
- 6 Click on the Files of Type drop-down menu and choose CSV or HTML.

- 7 Click on the Save button to save the report file and close the Save As form.
- 8 Close the RAN License Manager form.

Procedure 9-5 To recompute RAN license token consumption

Perform this procedure to resolve inconsistencies between the eNodeB parameter configuration and the RAN license token consumption in the 5620 SAM network.



Note 1 – Offline and online CM modifications that impact RAN license token consumption are blocked by the 5620 SAM until the recompute operation is complete.

Note 2 – The recompute operation does not complete if an NE is discovered by the 5620 SAM before the operation finishes.

- 1 Choose Administration→RAN License Manager from the 5620 SAM main menu. The RAN License Manager form opens with the General tab displayed.
- 2 Expand the Manual Licenses Recomputing panel, if required.
- 3 Click on the Recompute Licenses button. A dialog box appears.
- 4 Select the check box and click on the Yes button to start the recompute operation. The status of the recompute operation is displayed in the Recompute License Status field when the operation is complete.
- 5 Close the RAN License Manager form.

9.4 RAN license consumption management

This section describes the types of RAN license entitlements and how to manage token consumption of eNodeBs and cells in the managed network. Feature and capacity tokens are consumed when the appropriate parameters are configured on RAN devices using offline or online configuration. See Appendix B for information about the mapping between eNodeB parameter objects and RAN license entitlements.

Enumerated entitlements

Enumerated entitlements are consumed when you configure the corresponding enumerated parameters. Table 9-1 lists the objects that contain enumerated entitlement parameters and the applicable eNodeB versions.

Table 9-1 Enumerated entitlement parent objects

5620 SAM GUI name	LA3.0	TLA3.0	LA4.0	TLA4.0
Frequency And Bandwidth FDD	✓	—	✓	—
Frequency And Bandwidth TDD	—	✓	—	✓
Radio CAC eNodeB	—	—	✓	—
LTE Cell FDD	—	—	✓	—
Licensing Mngt System	—	—	✓	—

Feature entitlements

Feature entitlements are consumed when you configure the corresponding Boolean parameters on device objects, enabling or disabling the use of a feature. In the RAN license manager, feature entitlements correspond to parameter names and are prefixed by “LTE”. For example, LTEIsSonPciAllocationEnabled tokens are consumed by configuring the isSonPciAllocationEnabled parameter.

Table 9-2 lists the objects that contain feature entitlement parameters and the applicable eNodeB versions.

Table 9-2 Feature entitlement parent objects

5620 SAM GUI name	LA3.0	TLA3.0	LA4.0	TLA4.0
Activation Service	✓	✓	✓	✓
Cell Activation Service	—	—	✓	✓
Subscriber And Equipment Traces	✓	✓	✓	✓

Capacity entitlements

Capacity entitlements are currently deprecated and replaced by specific entitlements.

Specific entitlements

Specific entitlements are consumed when you configure the corresponding parameters on device objects. Specific entitlement token consumption is determined by a specific equation for each entitlement. Table 9-3 lists the supported specific entitlements, relevant parameter objects, and the equations that determine the token consumption.

Table 9-3 Specific entitlements

License name and parent object	Token consumption equals (rounded up)
maxNbOfCallCapacityLicensing Parent object: Radio CAC eNodeB	Per eNodeB: (maxNumberOfCallPerEnodeB ÷ 8)

(1 of 2)

License name and parent object	Token consumption equals (rounded up)
transmissionPowerCapacityLicensing Parent objects: Cell—cellDLTotalPower LTE Cell TDD/FDD—numberOfDLAntennas	Per LTE cell: $(10^{(0.1 \times \text{cellDLTotalPower} - 4)} \times \text{numberOfDLAntennas})$

(2 of 2)

RAN license consumption management procedures

Perform the following procedures to configure parameters that impact RAN license entitlement token consumption. See the *5620 SAM LTE Parameter Reference* for more information about the parameters that are described in the following procedures.



Note — Perform the procedures in section 9.3 in conjunction with the procedures in this section to verify that RAN license entitlements can accommodate additional token consumption and to ensure that RAN license violations do not occur.

Procedure 9-6 To configure license entitlement token consumption

This procedure provides general steps for configuring license-impacting parameters using online configuration. See chapter 7 for more information about online configuration.



Caution — Many license-impacting parameters are class A and B parameters. Configuring these parameters and saving the changes will cause full or partial device resets, which is service-affecting.



Note — See Appendix B for mapping information between eNodeB parameters and RAN license entitlements, and the object hierarchy of each license-impacting parameter for all supported eNodeB versions.

- 1 Choose one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
- 2 Click on the Components tab button.
- 3 Navigate to the required parameter parent object.



Note — Token consumption for some specific entitlements is calculated using more than one parameter. See Table 9-3 for more information.

- 4 Right-click on the object and choose Properties. The object form opens with the General tab displayed.

- 5 Configure license-impacting parameters, as required.
 - 6 Click on the OK button. The object form closes.
 - 7 Click on the OK button in the eNodeB NE Instance form. A dialog box appears.
 - 8 Click on the Yes button. The token consumption is updated and the device resets, if applicable.
-

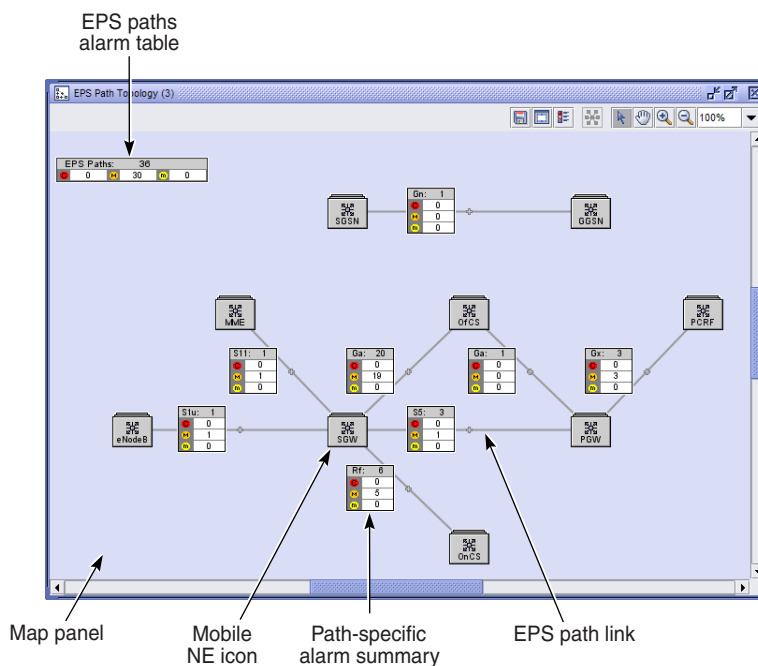
10 – LTE RAN EPS path management

- 10.1 EPS path topology map overview 10-2**
- 10.2 EPS peers and paths 10-9**
- 10.3 5620 SAM network topology maps 10-13**

10.1 EPS path topology map overview

The EPS path topology map displays a static representation of mobile network objects and EPS paths. Each network object icon represents an aggregate of all network objects of that type. For SGWs and PGWs, the icon represents an aggregate of all instances of that gateway type and all network objects that contain instances of that type. Each EPS path link represents an aggregate of all EPS paths of a specific type. Figure 10-1 shows the main elements of the mobility topology map.

Figure 10-1 EPS path topology map elements



20964

EPS path topology map window

The EPS path topology map window consists of:

- a titlebar
- a map panel that displays the network objects
- a map toolbar which consists of a collection of buttons that are used to manage the map view

The titlebar of the map window displays the following information:

- map type, which is EPS Path Topology in this case
- map number, which indicates the order in which the map was opened; for example, whether it is the first or the tenth map opened. There is no limit to the number of topology maps that you can have open at the same time.

EPS path topology map panel

The EPS path topology map panel displays a static map of the mobile network that contains:

- icons that represent an aggregate of the unmanaged mobile NEs and gateways
- icons that represent an aggregate of a mobile NE type or instance
- links between network elements that represent an aggregate of the EPS paths, such as S5
- an EPS path aggregated alarm table for each type of path
- an EPS aggregated alarm table for all EPS paths in the network; the table displays the total number of EPS paths and the number of paths that have at least one critical, major, and minor alarm
- icons that represent functions, such as the offline charging system

Selecting map objects

Click on the Select Tool button to select an object on the map. You can select multiple objects by pressing the Shift key and clicking on each object you need to select, or by drawing a selection rectangle around all of the objects you need to select on the topology map. You can select all of the NEs that are attached to an NE by selecting one or more NEs, right-clicking, and choosing Select Attached from the contextual menu. You can deselect a selected NE by pressing the CTRL key and clicking on the NE you need to deselect.

Moving map objects

You cannot move the map objects.

EPS path links

The map displays links that represent all EPS paths of a specific type between two mobile NEs or instances. You can right-click on a link to display a list of EPS paths.

Alarm tables

Each EPS path link is associated with an alarm table. There is also a path alarm table for the mobile network.

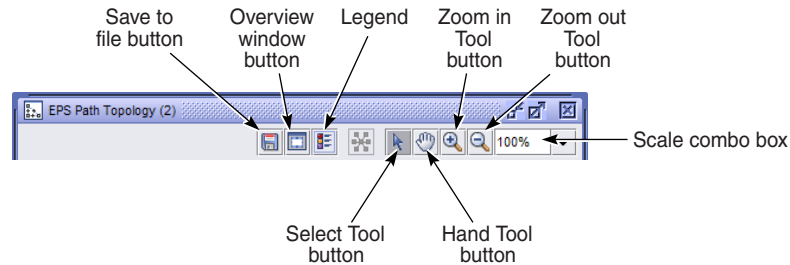
Zoom in and out using a mouse

The ability to zoom in and out on a map allows you to increase or decrease the size of the map. Use the mouse wheel to zoom in and zoom out of the map. Click on the map and roll the mouse wheel forward to zoom in or roll the mouse wheel backward to zoom out. Each roll of the mouse wheel brings the map objects closer or farther.

EPS path topology map toolbar

The EPS path topology map toolbar allows you to manage the view of the map. The toolbar appears above the map panel in the map window. Figure 10-2 shows the map toolbar and its elements.

Figure 10-2 Map toolbar elements



20965

Save To File button

Click on the Save To File button to save the map view or the full map. You can choose the location to save the map image and the file type. See Procedure 10-3 for more information about using the Save To File button. Figure 10-3 shows the Save To File button.

Figure 10-3 Save To File button

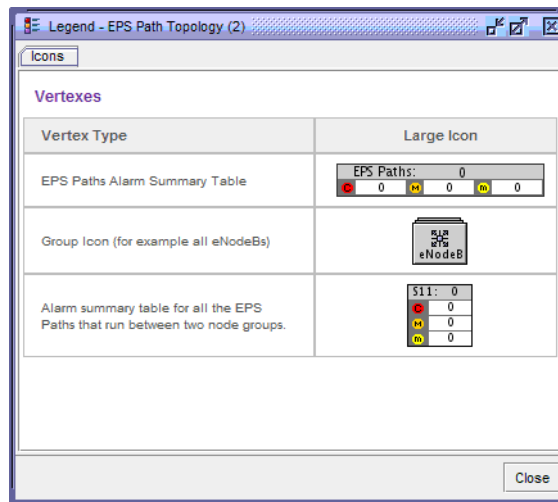


Overview Window button

Click on the Overview Window button to open the Overview window. Use the Overview window to pan the entire map and the area that you want to view.

Legend Tool button

Click on the Legend Tool button to open the Legend - EPS Path Topology window. The window contains a table that explains the meaning of the topology map icons. Figure 10-4 shows the Legend - EPS Path Topology display.

Figure 10-4 Legend - EPS Path Topology**Select Tool button**

Click on the Select Tool button to select an object on the map. You can select multiple objects by pressing the Shift key and clicking on each object you want to select, or by drawing a selection rectangle around all the objects you want to select on the mobility topology map.

Hand Tool button

Click on the Hand Tool button to switch to pan mode. Click and drag on the background to move the contents of the map in any direction.

Zoom in and zoom out using a Mouse or Tool buttons

The ability to zoom in and out on a map allows you to view details of the map. Click on the Zoom in Tool and Zoom out Tool buttons, and click on the map to resize the objects in a map or use the mouse wheel to zoom in and zoom out of topology maps. Click on the map and roll the mouse wheel forward to zoom in or roll the mouse wheel backward to zoom out. Each roll of the mouse wheel brings the map objects closer or farther.

Scale combo box

Use the scale combo box to increase or decrease the zoom in the map. You can choose a zoom percentage value from 25% to 300%, or fit all objects in the window from the drop-down menu. The scale combo box displays the current scale of the map.

EPS path topology map management procedures

Perform the following procedures to perform map management tasks.

Procedure 10-1 To open the EPS path topology map

- 1 Choose Application→EPS Path Topology from the 5620 SAM main menu.
- 2 The EPS path topology map appears.

See Procedure 10-2 for information about the map elements. See section 10.1 for information about the map view.

Procedure 10-2 To view EPS path topology map elements

- 1 Open an EPS path topology map, as described in Procedure 10-1. Figure 10-1 shows the map main elements.
- 2 View the NEs, links, and alarm tables, as required:
 - a View the EPS path topology map icons that represent mobile network NEs. Table 10-1 describes the map icons.

Table 10-1 EPS path topology map icons

Map icon type	Description
MME	Represents all of the managed MME devices and MME devices that have an EPS path to another NE. When you right-click on an MME icon, you can choose to display a list of all MME instances represented by the icon or all NEs that contain an MME instance. See the <i>5620 SAM LTE ePC User Guide</i> for more information about viewing MME properties.
SGW	Represents all of the managed SGW instances and all of the managed network elements that contain SGW instances. When you right-click on an SGW icon, you can choose to display a list of all gateway instances represented by the icon or all NEs that contain an SGW instance. See the <i>5620 SAM LTE ePC User Guide</i> for more information about configuring SGWs.
PGW	Represents all of the managed PGW instances and all of the managed network elements that contain PGW instances. When you right-click on a PGW icon, you can choose to display a list of all gateway instances represented by the icon or all NEs that contain a PGW instance. See the <i>5620 SAM LTE ePC User Guide</i> for more information about configuring PGWs.
PCRF	Represents all of the managed PCRF devices in the network and the PCRF devices that have an EPS path to another NE. When you right-click on a PCRF icon, you can choose to display a list of all DSC instances represented by the icon or all NEs that contain a DSC instance. See the <i>5620 SAM LTE ePC User Guide</i> for more information about viewing DSC properties.
GGSN	Represents the Gateway GPRS Support Node (GGSN) instances and all managed network elements that contain GGSN instances. When you right-click on a GGSN icon, you can choose to display a list of PGWs that are functioning as GGSNs.

(1 of 2)

Map icon type	Description
SGSN	Represents the Serving GPRS Support Node (SGSN) instances. When you right-click on an SGSN icon, you can choose to display a list of all unmanaged elements of type SGSN.
eNodeB	Represents all of the network elements of type eNodeB.
OfCS	Represents the offline charging system, a charging system where charging information does not affect, in real-time, the service being delivered.
OnCS	Represents the online charging system, a charging system where charging information can affect, in real-time, the service being delivered.

(2 of 2)

- b View the EPS path links. The EPS path links, which appear in the map between NEs, represent an aggregate of all of the EPS paths of a specific type. Right-click on a link and click on the menu item to display a list of all of the EPS paths that are represented by the link. You can choose a path from the list to view or modify the path properties.
- c View the EPS path alarm tables. Table 10-2 describes the EPS path alarm tables.

Table 10-2 EPS path alarm tables

Alarm table type	Description
EPS path-specific alarm tables	Each EPS path type is associated with an alarm table that is displayed over the path link on the map. Each alarm table displays the: <ul style="list-style-type: none"> • path type • total number of paths represented by the link • rows that display the number of paths with at least one critical, major, or minor alarm
EPS paths alarm table	There is one EPS paths alarm table associated with the topology map. The EPS paths alarm table displays the: <ul style="list-style-type: none"> • total number of paths of all types in the mobile network • total number of paths of all types that have at least one critical, major, or minor alarm

Procedure 10-3 To save a map view to a file

You can use the Save to File button to save a portion of a map or the entire map to the local file system. You can save the file to JPEG, JPG, BMP, and PNG formats.

- 1 Open an EPS path topology map, as described in Procedure 10-1.
- 2 Click on the Save To File button. The save options are displayed in the drop-down menu.

3 Choose an option from the drop-down menu:

- Choose Save Map View to save the current view.
- Choose Save Full Map to save the entire map view.

The Save form appears.

4 Save the results.

- i To choose a directory in which to save the listed information, configure the Save In parameter.
 - ii To create a filename, configure the File Name parameter.
 - iii Choose BMP, JPEG, JPG, or PNG from the File of Type drop-down menu.
 - iv Click on the Save button. The map view is saved to the specified file.
-

Procedure 10-4 To zoom in and zoom out of a map

- 1 Open an EPS path topology map, as described in Procedure 10-1.
 - 2 Perform one of the following:
 - a Use the mouse wheel to zoom in and zoom out. Click on the map. To zoom in, roll the mouse wheel forward. To zoom out, roll the mouse wheel backward.
 - b Click on the Zoom in Tool or Zoom out Tool button. Go to step 3.
 - 3 Move your cursor into the map panel. The icon changes to a magnifying glass that contains a + or - sign.
 - 4 Click on the area of the map you need to expand or contract. The map expands or contracts. Continue clicking until the required zoom level is reached.
 - 5 Use the opposite button and an equal number of clicks to return the map to the default setting.
 - 6 To return to the pointer icon, click on the Select Tool button in the toolbar.
-

Procedure 10-5 To view and modify EPS path information

- 1 Open an EPS path topology map, as described in Procedure 10-1.
 - 2 To list EPS paths, perform one of the following.
 - a Using an EPS path link:
 - i Right-click on the EPS path link for the type of path that you need to list.
 - ii Click on the displayed menu item. An EPS paths form opens that displays a list of paths.
 - iii Choose a path from the list and click on the Properties button. The properties edit form for the EPS path opens.
 - b Using the EPS path alarm table:
 - i Right-click on the EPS path alarm table at the top of the EPS path topology map.
 - ii Click on the menu item. The EPS Paths form opens.
 - iii Click on the Select Object Type button and choose the type of path from the list.
 - iv Click on the Search button. A list of paths appears.
 - v Choose a path from the list and click on the Properties button. The path type edit form opens.
 - 3 View and modify the path information, as required.
 - 4 Close the path edit form.
 - 5 Close the EPS paths form.
-

10.2 EPS peers and paths

The 5620 SAM allows you to view the status, statistics, state, and faults associated with the EPS peers and paths.

Each peer or path combines a pair of matching reference points and peer objects of two ePC nodes in a managed entity. Reference points are based on the LTE 3GPP standard, and are created automatically when you configure an LTE node such as an SGW or a PGW. EPS paths are created dynamically when LTE peer devices are signaled. After the 5620 SAM resynchronizes a control session, the EPS peers and EPS paths are discovered by the 5620 SAM.

EPS peers

EPS peers are neighboring nodes that share the endpoints of an EPS path. An example is an S5 EPS path: one endpoint is always an SGW and the other endpoint is always a PGW. The PGW and the SGW are EPS peers.

The 5620 SAM supports the following types of peers:

- diameter-based
- GTP/PMIP-based

EPS paths

An EPS path is a point-to-point connection between LTE nodes that is used for bearer control. EPS paths include:

- eNodeB to SGW (S1-U path)
- SGW to PGW (S5 path)
- SGW to MME (S11 path)
- PGW to PCRF (Gx path)
- SGW to CCF (Rf path)

The 5620 SAM allows you to discover and list all of the EPS paths in the entire mobile network or on a specific node. You can filter using specific parameters, such as type, status, and IP address, to display specific bearer paths.

EPS paths are single-sided or double-sided:

- single-sided—the 5620 SAM manages only one endpoint, such as the following:
 - S11 path between the SGW and the MME, where only the SGW is managed by the 5620 SAM
 - Gx path between the PGW and the PCRF, where only the PGW is managed by the 5620 SAM
 - S1-U path between the SGW and the eNodeB, where only the SGW is managed by the 5620 SAM
 - Rf path between the SGW and the CFF, where only the SGW is managed by the 5620 SAM
- double-sided—the 5620 SAM manages both endpoints, such as the S5 interface between the SGW and PGW, where both gateways are managed by the 5620 SAM

Procedures

The following procedures describe how to view the properties of EPS peers and paths.

Procedure 10-6 To view the properties of EPS peers from the EPS Peers and Paths form

- 1 Choose Manage→Mobile Core→EPS Peers and Paths from the 5620 SAM main menu. The Manage EPS Peers and Paths form opens.
- 2 Choose Evolved Packet Solution Peer (LTE) from the Select Object Type drop-down menu. The supported types of peers appear as subtending objects in the Evolved Packet Solution Peer (LTE) navigation tree.
- 3 Perform one of the following to choose a type of peer from the drop-down menu:
 - a Diameter Based Peer (LTE)
 - AGW Diameter Peer (LTE)
 - Gx AGW Peer (LTE)
 - Rf AGW Peer (LTE)
 - DSC Diameter Peer (LTE)
 - b GTP/PMIP Based Peer (TLE)
 - AGW GTP/PMIP Peer (LTE)
 - S11 SGW Peer (LTE)
 - S1u SGW Peer (LTE)
 - S5 AGW Peer (LTE)
 - S8 AGW Peer (LTE)
 - MME GTP/PMIP Peer (LTE)
 - Gn MME Peer (LTE)
 - S10 MME Peer (LTE)
 - S11 MME Peer (LTE)
 - S13 MME Peer (LTE)
 - S1mme MME Peer (LTE)
 - S3 MME Peer (LTE)
 - S6a MME Peer (LTE)
 - SG MME Peer (LTE)
 - Sv MME Peer (LTE)
- 4 Configure the filter criteria, if required, and click on the Search button. The form lists the available EPS peers.
- 5 Choose an EPS peer from the list and click on the Properties button. The EPS Peer form opens with the General tab displayed.

- 6 Click on the following tab buttons for additional information:
 - Diameter—lists the Diameter management state, detailed state, profile name, and profile index. This tab applies only to Gx and Rf peers.
 - Statistics—lists the statistics associated with the peer
 - Faults—lists the faults associated with the EPS peer according to the following alarm types:
 - Object Alarms
 - Affecting Alarms
 - Aggregated Alarms
 - Alarms on related Objects
 - 7 Click on the Cancel button to close the form.
-

Procedure 10-7 To view the properties of EPS paths from the EPS Peers and Paths form

- 1 Choose Manage→Mobile Core→EPS Peers and Paths from the 5620 SAM main menu. The Peers and Paths form opens.
- 2 Choose Evolved Packet Solution Path (LTE) from the Select Object Type drop-down menu. The following supported paths appear as subtending objects in the Evolved Packet Solution Path (LTE) navigation tree:
 - Gx Path (LTE)
 - Rf Path (LTE)
 - S11 Path (LTE)
 - S1u Path (LTE)
 - S5 Path (LTE)
- 3 Configure the filter criteria, if required, and click on the Search button. The form lists the available EPS paths.
- 4 Choose an EPS path from the list and click on the Properties button. The EPS Path properties form opens with the General tab displayed.

- 5 Click on the following tab buttons for additional information:
 - Tree—lists the component tree that is associated with the path
 - Drill Down—see the *5620 SAM LTE ePC User Guide* for more information about how to perform the manual drill-down operation. Drill-down is not supported on the Rf EPS paths.
 - Components—this tab is populated only after the drill-down operation is performed
 - Discovery Log—a log appears if the drill-down operation fails
 - Faults—lists the faults associated with the EPS path according to the following alarm types:
 - Object Alarms
 - Affecting Alarms
 - Aggregated Alarms
 - Alarms on related Objects
 - 6 Click on the Cancel button to close the form.
-

10.3 5620 SAM network topology maps

The 5620 SAM uses map windows to visually represent network objects and pathways. Each map displays network objects and information, and provides contextual menus to open forms that display additional information. See the *5620 SAM User Guide* for more information about generic tasks for physical topology management.

11 – LTE RAN security

11.1 Overview	11-2
11.2 Workflow to configure LTE RAN security	11-2
11.3 5620 SAM user and group security	11-2
11.4 RAN sharing	11-4
11.5 eNodeB IPsec	11-15

11.1 Overview

The 5620 SAM provides security functions for user groups, devices, and paths. User security functions define 5620 SAM user group access to objects in the managed network. The 5620 SAM eNodeB IPsec functions facilitate the configuration of IPsec parameters for managed eNodeBs.

This chapter provides information about 5620 SAM security functions that apply to LTE RAN management only. For more information about the security functions the 5620 SAM, see the *5620 SAM User Guide*.

11.2 Workflow to configure LTE RAN security

- 1 Configure 5620 SAM user security to allow for secure RAN sharing. See section [11.4](#) for more information.
 - i Create equipment groups and populate the groups with shared eNodeBs. See Procedures [11-1](#) and [11-2](#).
 - ii Create scope of command roles and scope of command profiles for delegate operators. See Procedures [11-3](#) and [11-4](#).
 - iii Create spans of control and span of control profiles for delegate operators. See Procedures [11-5](#) and [11-6](#).
 - iv Create user groups and user accounts for delegate operators and assign both a scope of command profile and a span of control profile to a user group. See Procedures [11-7](#) and [11-8](#).
 - v Create discovery rules for RAN sharing to automatically add eNodeBs to shared equipment groups and spans when the NEs are discovered by the 5620 SAM. See Procedure [5-6](#).
 - vi Repeat steps [1 i](#) to [v](#), as required, for additional NEs, MNOs, and delegate operators.
 - vii Suspend or reinstate user accounts, as required. See Procedure [11-11](#).
- 2 Enable or disable IPsec for eNodeBs. See Procedure [11-12](#).

11.3 5620 SAM user and group security

You can use the 5620 SAM to configure user accounts, user groups, and scope of command to configure user access over GUI or OSS interface. This section describes user and group security functions that are specific to RAN management with the 5620 SAM.

Scope of command

A scope of command profile is a collection of one or more roles that define the functions that the user is allowed to perform in the 5620 SAM network. Scope of command profiles can be used to create user groups with restricted permissions in order to maintain the security of the managed network.

Table 11-1 lists the scope of command roles that are relevant to RAN management with the 5620 SAM. See the *5620 SAM User Guide* for a complete list of predefined scope of command roles in the 5620 SAM.

Table 11-1 Scope of command roles specific to RAN management

Role	Access Provided	Role ID
Network Element Software Management	Router administration (Backup and Restore, Scheduling, Backup Policies, Upgrade Policies, Deployment Policies, and Management Ping Policies), Backup Files, Software Images, and the ability to use invoke Telnet to the node from the 5620 SAM.	13
OSS Management	The ability to use 5620 SAM-O.	19
Work Order Activation ⁽¹⁾	The ability to perform CM workorder activation.	31
Configuration Snapshot Export	The ability to export CM configuration snapshots.	32
Create and Delete Access	The ability to create and/or delete eNodeB objects via 5620 SAM-O.	33
Configuration Management which causes node reset ⁽²⁾	The ability to configure objects which causes a full or partial reset of the node.	34
eNodeB NEM Operator	The ability to launch the 9400 NEM from the 5620 SAM client application.	36

Notes

- ⁽¹⁾ This role provides all configuration permissions for eNodeB management, such as create and delete access, and configuration actions that cause a reset of the NE. Access to this role must be strictly managed.
- ⁽²⁾ This role must be used in conjunction with a role that contains the *lte* permission, such as Network Element Software Management.

The following scope of command roles provide access for configuration actions over OSS interface that do not cause a reset of the NE:

- Create and Delete Access
- OSS Management
- Network Element Software Management

The following scope of command roles provide access for configuration actions over OSS interface that cause a partial or full reset of the NE:

- Create and Delete Access
- OSS Management
- Network Element Software Management
- Configuration Management which causes node reset



Note — The Network Element Software Management role contains the *lte* permission. Customized scope of command roles that also contain the *lte* permission can be substituted, if required.

11.4 RAN sharing

The user security functions of the 5620 SAM provide a comprehensive level of object and NE access control that allows the configuration of secure RAN sharing between MNOs and across PLMNs. MNOs that have restricted access shared NEs and cannot access the general managed network or administrative functions are called *delegate operators*. Network administrators must ensure that 5620 SAM user security settings are configured to provide delegate operators with sufficient access to shared NEs but prevent access to unshared parts of the managed network and administrator functions. This section describes the workflow and procedures that are required for RAN sharing in the 5620 SAM network.

The network administrator, or a user with access to the security package, must configure the following user security functions and network objects for RAN sharing:

- equipment groups, which contain shared NEs, that represent the only network resources that delegate operators can access
- scope of command roles that contain a task-based set of permissions for objects in the network, and scope of command profiles that contain one or more scope of command roles
- spans of control that specify a set of managed network objects that delegate users can access, and span of control profiles that contain one or more spans of control
- user accounts and groups that are associated with a scope of command profile and a span of control profile

See section [11.2](#) for a workflow of the tasks that are required to configure 5620 SAM user security for RAN sharing.

RAN sharing - scope of command

Scope of command roles and profiles for RAN sharing must be configured with the appropriate permissions for RAN devices in order to provide delegate operators with a sufficient level of control over shared NEs. Table [11-1](#) describes the default roles for RAN management that are created when the 5620 SAM server is installed.

MNO user accounts must have restricted scope of command roles that do not contain access to the following administrator functions:

- activation manager
- snapshot manager
- backup policies
- software upgrade policies
- eNodeB software upgrade operations
- eNodeB backup and restore

In order to prevent access to administrator functions, do not assign the Work Order Activation, Configuration Snapshot Export, or Network Element Software Management scope of command roles to MNO user accounts.

Table 11-2 describes the permissions that are required for RAN sharing as an example to help with role creation. More permissions may be required depending on the planned complexity of RAN sharing in the 5620 SAM network. See the Appendix A of the *5620 SAM User Guide* for a list of assignable permissions and default scope of command roles in the 5620 SAM.

Table 11-2 Permissions required for RAN sharing

Permission (package.class)	Description
lte	LTE - All LTE configurations and status.
impact.FullReset	Full Reset - Ability to configure objects which will result in a full reset of the node. Currently applies to the 9412 eNodeB.
impact.PartialReset	Partial Reset - Ability to configure objects which will result in a partial reset of impacted SW/HW unit. Currently applies to the 9412 eNodeB.

RAN sharing and the 5620 SAM Supervision Module

You can use the 5620 SAM Supervision Module to monitor shared NEs by including spans that are created for RAN sharing in supervision groups and summary views. See the *5620 SAM Supervision Module User Guide* for more information.

RAN sharing procedures

The procedures in this section describe how to configure the 5620 SAM with the users, equipment groups, spans of control, and scope of command roles that are required for secure RAN sharing. See the *5620 SAM Parameter Guide* for descriptions of the parameters that are described in the following procedures.



Note 1 — The following procedures must be performed as the 5620 SAM admin user.

Note 2 — See the *5620 SAM User Guide* for more information about 5620 SAM user security, including RADIUS and TACACS+ authentication.

Procedure 11-1 To create an equipment group

Perform this procedure to create an equipment group that will contain eNodeBs for RAN sharing. If there is a span of control for RAN sharing, you can add the equipment group to the span of control in this procedure. Otherwise, you can create a span of control by performing Procedure 11-5 and adding the equipment group created in this procedure.



Note — Equipment groups are also called topology groups.

- 1 Perform one of the following to open the Group (Create) form:
 - a Choose Create→Equipment→Group from the 5620 SAM main menu.
 - b Right-click on the network object in the Equipment view of the navigation tree and choose Equipment→Create Group from the contextual menu.



Note — You can create an equipment group within an equipment group by right-clicking on the equipment group object instead of the network object.

- 2 Configure the parameters:
 - Group Name
 - Description
 - Background Image
 - 3 Click on the Apply button. The equipment group is created. An object for the equipment group is displayed in the equipment navigation tree and on the appropriate topology maps.
 - 4 Add the equipment group to a span of control, if required:
 - i Click on the Spans tab button.
 - ii Click on the Add button. The Select Span(s) - Equipment Group form opens with a list of available spans.
 - iii Select one or more spans to apply to the topology group.
 - 5 Click on the OK button. A dialog box appears.
 - 6 Click on the Yes button and close the Select Span(s) - Equipment Group form.
-

Procedure 11-2 To add NEs to an equipment group



Note — An equipment group can contain a maximum of 500 NEs.

- 1 Choose Application→Physical Topology, or Service Tunnel Topology from the 5620 SAM main menu. The appropriate map window opens.
- 2 Populate equipment groups, as required:
 - a Click on a map object, such an NE, in the map window and drag the object to the equipment group that you need the map object to belong. The map object becomes a descendent object of the equipment group.
 - b Click on an NE object in the equipment window and drag the object onto the equipment group to which you need the NE object to belong. The NE object becomes a descendent object of the equipment group.

Procedure 11-3 To create a scope of command role

The scope of command role specifies the permissions that MNO delegate users have on the 5620 SAM network. Verify that the permissions are sufficient, and do not compromise the security of the network.

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
- 2 Click on the Scope of Command tab button.
- 3 Click on the Create button and choose Role. The Role (Create) form opens with the General tab displayed.
- 4 Configure the parameters:
 - Auto-Assign ID
 - Role ID
 - Description
- 5 Click on the Permissions tab button. A list of the 5620 SAM packages, methods, and classes is displayed.



Note — When you enable the Create permission for a 5620 SAM package, method, or class, the Update/Execute permission is automatically enabled.

When you enable the Update/Execute permission for a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

- 6 Select the required access permissions that you need to assign to the scope of command role.
 - 7 Click on the OK button to save the role and close the Role (Create) form.
 - 8 Close the 5620 SAM User Security - Security Management (Edit) form.
-

Procedure 11-4 To create a scope of command profile

Perform this procedure to create a scope of command profile that contains scope of command roles for RAN sharing. Perform Procedure [11-3](#) to create a scope of command role.

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
 - 2 Click on the Scope of Command tab button.
 - 3 Click on the Create button and choose Profile. The Scope of Command Profile (Create) form opens with the General tab displayed.
 - 4 Configure the parameters:
 - Auto-Assign ID
 - Profile ID
 - Profile Name
 - Description
 - 5 Assign one or more scope of command roles to the profile.
 - i Click on the Roles tab button.
 - ii Click on the Add button. The Select Scope Of Command Role(s) - Scope Of Command Profile form opens.
 - iii Select one or more roles and click on the OK button. The Select Scope of Command Role(s) - Scope Of Command Profile form closes and the selected roles are added to the list.
 - iv Click on the OK button. The Scope of Command Profile (Create) form closes.
 - 6 Close the 5620 SAM User Security - Security Management (Edit) form.
-

Procedure 11-5 To create a span of control

You can limit delegate operator access to a specific subset of NEs by only adding the equipment groups created in Procedure 11-1.

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
- 2 Click on the Span of Control tab button.
- 3 Click on the Create button and choose Span. The Span (Create) form opens with the General tab displayed.
- 4 Configure the parameters:
 - Auto-Assign ID
 - Span ID
 - Span Name
 - Description
- 5 Click on the Contents tab button.
- 6 Click on the Add button and choose Equipment Group. The Select Equipment Group form opens.
- 7 Select one or more equipment groups and click on the OK button. The Select Equipment Group form closes and the objects are listed on the Span (Create) form.



Note — Delegate users can view objects that are not assigned to a span. Ensure that all restricted NEs and NE groups, including the Network, Discovered NEs, and Pre-Provisioned NE groups are assigned to spans and that these spans are not available to delegate users.

- 8 Click on the OK button. The Span (Create) form closes.
 - 9 Close the 5620 SAM User Security - Security Management (Edit) form.
-

Procedure 11-6 To create a span of control profile

A span of control profile contains one or more spans of control that specify the network objects that delegate users can access, and an access level for each span. Perform Procedure 11-5 to create a span of control.

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 Click on the Span of Control tab button.
- 3 Click on the Create button and choose Profile. The Span of Control Profile (Create) form opens with the General tab displayed.

- 4 Configure the parameters:
 - Auto-Assign ID
 - Profile ID
 - Profile Name
 - Description
- 5 Click on the Spans tab button. A list of default spans with View access is displayed.
- 6 Perform one the following steps to delete default spans from the profile, if required:



Note — Deleting the default spans will prevent the delegate users from being able to view objects in the default spans. Alcatel-Lucent recommends deleting all default spans from span of control profiles for RAN sharing.

- a To delete all default spans from the profile:
 - i Select all of the spans by clicking on an object and pressing CTRL+A.
 - ii Click on the Delete button.
 - b To delete one or more default spans from the profile:
 - i Select one or more spans. To select multiple spans of control, hold down the CTRL key and click on the spans.
 - ii Click on the Delete button.
- 7 Click on the Add button and choose an access type. The Select *access_type* Spans form opens.
 - 8 Select one or more spans in the list and click on the OK button. The Select *access_type* form closes and the selected spans are listed in the span of control profile.



Note — All discovered NEs are added to the default router span and cannot be removed. Providing view or edit access to the default router span will give delegate operators access to all NEs in the managed network. Blocking view or edit access will block access for all NEs in the managed network, including shared NEs.

- 9 Click on the OK button to save the span of control profile and close the Span of Control (Create) form.
 - 10 Close the 5620 SAM User Security - Security Management (Edit) form.
-

Procedure 11-7 To create a 5620 SAM user group

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
- 2 Click on the User Groups tab button.
- 3 Perform one of the following:
 - a Create a user group by clicking on the Create button. The User Group (Create) form opens with the General tab displayed.
 - b Modify a user group:
 - i Configure the filter criteria, if required, and click on the Search button. A list of groups is displayed.
 - ii Select a group and click on the Properties button. The User Group (Edit) form opens with the General tab displayed.
- 4 Configure the parameters:

• User Group	• Account Expiry
• Description	• Password Expiry
• User Group State	• Override Global Timeout
• Apply Local Authentication Only	• Client Timeout (minutes)
• Maximum User Sessions Allowed	
- 5 If the user group is intended for remote users, configure the parameters:
 - Maximum GUI Sessions Allowed
 - Maximum OSS Sessions Allowed
 - Priority
- 6 Assign a scope of command profile to the user group.
 - i Click on the Select button in the Scope of Command panel. The Select Scope of Command Profile form opens.
 - ii Select a profile in the list and click on the OK button. The Select Scope of Command Profile form closes, and the User Group (Create) form displays the scope of command profile name.
- 7 Assign a span of control profile to the user group.
 - i Click on the Select button in the Span of Control panel. The Select Span of Control Profile form opens.
 - ii Select a profile in the list and click on the OK button. The Select Span of Control Profile form closes, and the User Group (Create) form displays the span of control profile name.

- 8 If you are creating a user group:
 - i Click on the OK button. The User Group (Create) form closes.
 - ii Go to step 15.
- 9 Click on the Format and Range Policies tab button.
- 10 Click on the Add button. The Select Format or Range Policies form opens.
- 11 Select one or more policies in the list and click on the OK button.
- 12 Click on the OK button. A dialog box appears.



Note — When you change the scope of command or span of control profiles of a group and apply the changes, the permissions of each user in the group are changed immediately.

- 13 Click on the Yes button. The User Group (Create) form closes.
 - 14 If an active client GUI session is affected by the user group modification, restart the GUI client.
 - 15 Close the 5620 SAM User Security - Security Management (Edit) form.
-

Procedure 11-8 To create a 5620 SAM user account

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 Click on the Users tab button.
- 3 Perform one of the following:
 - a Create a user account by clicking on the Create button. The User (Create) form opens with the General tab displayed.
 - b Modify a user account:
 - i Configure the filter criteria, if required, and click on the Search button. A list of user accounts is displayed.
 - ii Select an account in the list and click on the Properties button. The User (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- | | |
|----------------------------|--------------------------------|
| • User Name | • User Password |
| • Description | • Confirm Password |
| • User State | • Maximum Sessions Allowed |
| • E-mail Address | • Maximum OSS Sessions Allowed |
| • Priority | • Valid Client IP address |
| • Password Change Required | • Enable IP Address validation |



Note — If the user account is for a remote user, you cannot configure the Maximum Sessions Allowed, Maximum OSS Sessions Allowed, or Priority parameters. For remote users, these parameters are derived from the user group that is configured on the user account.

5 To test the validity of the user e-mail address, click on the Test E-mail button beside the E-mail Address parameter.



Note — Before you test the validity of the user e-mail address, ensure that the outgoing SMTP e-mail server and e-mail test message are configured. See the *5620 SAM User Guide* for more information.

6 Choose a user group for the user account:

- i Click on the Select button. The groupName form opens.
- ii Select a user group in the list and click on the OK button. The groupName form closes, and the User (Create) form displays the user group name.

7 If you are creating a user account:

- i Click on the OK button. The User Group (Create) form closes.
- ii Go to step 13.

8 Click on the Format and Range Policies tab button.

9 Click on the Add button. The Select Format or Range Policies form opens.

10 Select one or more policies in the list and click on the OK button.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The User (Edit) form closes.

13 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 11-9 To copy a 5620 SAM user account

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
 - 2 Click on the Users tab button.
 - 3 Set the filter criteria and click on the Search button. A list of configured users opens.
 - 4 Select a user from the list and click on the Properties button. The User *type_of_user*, Group *user_group* (Edit) form opens.
 - 5 Click on the Copy button. A User (Create) form opens for the second user.
 - 6 Configure the parameters, as required. You must change the User Name parameter, and configure the User Password and Confirm Password parameters.
 - 7 Click on the OK button to save the changes and close the User (Create) form.
 - 8 Close the 5620 SAM User Security - Security Management (Edit) form.
-

Procedure 11-10 To search for inactive user accounts

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
 - 2 Click on the Users tab button.
 - 3 Click on the Inactive User Search button and perform one of the following.
 - a Choose 90 Days.
 - b Choose 180 Days.
 - c Choose Custom. The User Inactivity Period form opens.
 - i Enter a value for User inactive greater than or equal to.
 - ii Click on the OK button to close the form and return to the Inactive User Search form.
 - 4 User accounts that have been inactive for a number of days that is greater than or equal to the value entered in step 3 are displayed.
 - 5 Perform actions for inactive user accounts, as required.
-

Procedure 11-11 To suspend or reinstate a 5620 SAM user account

- 1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
 - 2 Click on the Users tab button.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of users is displayed.
 - 4 Select a user and click on the Properties button. The User (Edit) form opens.
 - 5 Perform the following steps to suspend or re-instate the user:
 - a To suspend the user, click on the User State parameter and choose Suspended.
 - b To reinstate the user, click on the User State parameter and choose Active.
 - 6 Click on the OK button. A dialog box appears.
 - 7 Click on the Yes button and close the User (Edit) form.
 - 8 Close the 5620 SAM User Security - Security Management (Edit) form.
-

11.5 eNodeB IPsec

The eNodeB IP security function protects all or part of the traffic of an eNodeB by routing OAM and inter-device traffic through a SEG and protected subnets. You must configure the SEG before you can use IPsec with the eNodeB. You can configure IPsec parameters using online or offline configuration.

IPsec procedures

Perform the following procedures to configure IPsec on the eNodeB using the 5620 SAM. See the *5620 SAM LTE Parameter Reference* for more information about the parameters described in the following procedures.

Procedure 11-12 To enable or disable IPsec on an eNodeB



Caution — Enabling or disabling IPsec causes a full reset of the NE, which is service-affecting.



Note — Enabling the IPsec feature on an eNodeB consumes a RAN license feature entitlement token.

- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
 - 2 Click on the Components tab button.
 - 3 Navigate to the Activation Service object. The path is eNodeB NE Instance→Activation Service→Activation Service ID *n*.
 - 4 Right-click on the Activation Service object and choose Properties from the contextual menu. The Activation Service form opens.
 - 5 Configure the isIPsecEnabled parameter to enable or disable IPsec on the eNodeB.
 - 6 Click on the OK button to close the form and return to the eNodeB NE Instance form.
 - 7 Click on the Apply button. A dialog box appears.
 - 8 Click on the Yes button. The changes to the Activation Service object are saved, the device resets, and RAN license token consumption is updated.
 - 9 Close the eNodeB NE Instance form.
-

12 – LTE RAN SON management

12.1 Overview 12-2

12.2 Workflow to configure SON functions 12-2

12.3 ANR 12-2

12.4 PCI 12-7

12.1 Overview

The Self Organizing Network is a function of the LTE RAN that allows operators to focus time and effort on the macro level of network administration while built-in algorithms automatically negotiate optimal inter-device settings and pathways at the micro level. You can use the 5620 SAM to enable and configure the following SON functions for eNodeBs using online and offline configuration:

- ANR
- IRAT ANR
- PCI

12.2 Workflow to configure SON functions

Perform the following steps to manage eNodeB SON features using the 5620 SAM.

- 1 Enable or disable ANR on eNodeBs. See Procedure [12-1](#).
- 2 Enable or disable IRAT ANR on eNodeBs. See Procedure [12-2](#).
- 3 Reset ANR on eNodeBs, as required. See Procedure [12-3](#).
- 4 Configure inter-LTE ANR parameters on eNodeBs. See Procedure [12-4](#).
- 5 Configure PCI for eNodeBs, as required.
 - i Enable or disable PCI on eNodeBs. See Procedure [12-6](#).
 - ii Configure PCI parameters. See Procedure [12-7](#).

12.3 ANR

ANR is a cyclical function that operates on a per-cell basis in active and dormant phases to automatically optimize neighbor relations between eNodeBs and cells. The ANR function allows eNodeBs to automatically detect the optimal signal strength between neighboring eNodeBs and establish X2 interfaces in order to provide the best possible conditions for HO of UE. The discovery of eNodeB neighbor relations via the ANR function results in the creation of X2 connections that are managed by the 5620 SAM.

You can configure whitelisting and blacklisting to complement the automatic calculation of neighbor relations between specific eNodeBs. Whitelisted X2 connections are established as permanent connections between eNodeBs and are not removed by the ANR function. Blacklisted X2 connections are prevented from inclusion as valid neighbor relations.

Enabling or disabling the ANR function has a direct impact on the automatic PCI allocation feature. When you disable the ANR feature for a RAN device, the 5620 SAM displays a warning message that indicates the impact on the PCI allocation. See table [12-1](#) for more information about the relationship between ANR and PCI functions.

Table 12-1 ANR and PCI relationship

ANR enabled	PCI enabled	PCI distributed	Comment
False	False	False	N/A
False	True	False	Check is done by device
True	False	False	N/A
True	True	True	N/A



Note 1 – The 5620 SAM will prevent offline and online configuration changes on LA2.0 or TLA2.1 eNodeBs when ANR is enabled on the device, with the exception of setting ANR to disabled. Perform Procedure 12-1 to manually enable or disable ANR on an eNodeB.

Note 2 – Configuration changes are permitted on all eNodeB versions other than LA2.0 and TLA2.1 when ANR is enabled on the device.

Note 3 – When you lock a cell that is running an active ANR phase, the phase is suspended until you unlock the cell.

IRAT ANR

IRAT ANR is a SON function for neighbor relations across radio technologies, such as LTE and UTRAN. You can configure the IRAT ANR parameters of eNodeBs using the 5620 SAM.



Note – IRAT ANR is supported on eNodeB version LA4.0.

ANR procedures

Perform the following procedures to configure the ANR function of eNodeBs. See the *5620 SAM LTE Parameter Reference* for descriptions of the parameters in the following procedures.

Procedure 12-1 To enable or disable the ANR function on an eNodeB



Note – Enabling the ANR function on an eNodeB consumes a RAN license feature entitlement token.

- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.

- 2 Click on the Components tab button.
 - 3 Navigate to the Activation Service object. The path is eNodeB NE Instance→Activation Service→Activation Service ID *n*.
 - 4 Right-click on the Activation Service ID *n* object and choose Properties from the contextual menu. The Activation Service (Edit) form opens.
 - 5 Choose one of the following:
 - a To enable or disable ANR for LA3.x and below, configure the anrEnable parameter.
 - b To enable or disable ANR for LA4.0, configure the lteIntraFrequencyAnrEnabled parameter.
 - 6 Click on the OK button to close the form and return to the eNodeB NE Instance form.
 - 7 Click on the Apply button. A confirmation form appears.
 - 8 Click on the Yes button to confirm the changes and close the confirmation form. The changes to the Activation Service object are saved and RAN license token consumption is updated.
 - 9 Close the eNodeB NE Instance form.
-

Procedure 12-2 To enable or disable the IRAT ANR function on an eNodeB

- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
- 2 Click on the Components tab button.
- 3 Navigate to the Activation Service object. The path is eNodeB NE Instance→Activation Service→Activation Service ID *n*.
- 4 Right-click on the Activation Service ID *n* object and choose Properties from the contextual menu. The Activation Service (Edit) form opens.
- 5 Configure the ultraAnrEnabled parameter.
- 6 Click on the OK button to close the form and return to the eNodeB NE Instance form.
- 7 Click on the Apply button. A confirmation form appears.

- 8 Click on the Yes button to confirm the changes and close the confirmation form. The changes to the Activation Service object are saved and RAN license token consumption is updated.
 - 9 Close the eNodeB NE Instance form.
-

Procedure 12-3 To manually reset ANR and IRAT ANR on an eNodeB



Caution — Resetting an active ANR cycle is service-affecting.

- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
 - 2 Choose one of the following:
 - a To reset ANR, perform the following steps:
 - i Click on the Reset ANR button in the Automatic Neighbor Relation State panel. A dialog box appears.
 - ii Select the check box to acknowledge the warning.
 - iii Click on the Yes button.
 - b To reset IRAT ANR, perform the following steps:
 - i Click on the Reset Utra ANR button in the Automatic Neighbor Relation State panel. A dialog box appears.
 - ii Select the check box to acknowledge the warning.
 - iii Click on the Yes button.
 - 3 Monitor ANR calculation status, as required.
 - 4 Close the eNodeB NE Instance form.
-

Procedure 12-4 To configure inter-LTE ANR parameters for neighbor relations

Perform this procedure to configure LTE neighboring cell relation objects, including blacklisting and whitelisting parameters, for eNodeBs.

- 1 Choose Manage→Mobile Access→eNodeB Logical Objects from the 5620 SAM main menu.
 - 2 Choose LTE Neighboring Cell Relation (LTE) from the object drop-down list.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of LTE Neighboring Cell Relation objects is displayed.
 - 4 Select an object from the list and click on the Properties button. The LTE Neighboring Cell Relation (Edit) form opens with the General tab displayed.
 - 5 Choose one of the following, depending on the eNodeB version:
 - a For LA2.x eNodeBs, configure the following parameters:
 - noRemove
 - noHO
 - b For LA3.x-LA4.x eNodeBs, configure the following parameters:
 - noRemove
 - noHoOrReselection
 - 6 Click on the Apply button. A dialog box appears.
 - 7 Click on the Yes button.
 - 8 Click on the Properties button in the X2 Access ID Pointer panel. The eNodeB X2 Reference Point (Edit) form opens with the General tab displayed.
 - 9 Configure the parameters:
 - noRemove
 - noX2
 - noX2HO
 - 10 Click on the OK button. A dialog box appears.
 - 11 Click on the Yes button. The form closes and the changes are saved.
 - 12 Close the forms, as required.
-

Procedure 12-5 To configure IRAT ANR parameters for neighbor relations

Perform this procedure to configure IRAT neighboring cell relation objects, including blacklisting and whitelisting parameters, for eNodeBs.

- 1 Choose Manage→Mobile Access→eNodeB Logical Objects from the 5620 SAM main menu.
 - 2 Choose UTRAN FDD Neighboring Cell Relation (LTE) from the object drop-down list.
 - 3 Configure the filter criteria, if required, and click on the Search button. A list of UTRAN Neighboring Cell Relation objects is displayed.
 - 4 Select an object from the list and click on the Properties button. The UTRAN FDD Neighboring Cell Relation (Edit) form opens with the General tab displayed.
 - 5 Configure the parameters:
 - noRemove
 - noHoOrReselection
 - 6 Click on the OK button. A dialog box appears.
 - 7 Click on the Yes button. The form closes and the changes are saved.
 - 8 Close the forms, as required.
-

12.4 PCI

The PCI of an LTE cell identifies the cell for detection by UE and inclusion in the ANR function of eNodeBs. The PCI of an eNodeB is generally predetermined with the aid of a RAN planning tool and configured via WO with the 9952 WPS. The 5620 SAM resynchronizes PCI designations in the event that a PCI conflict causes the PCI of an LTE cell to change. Perform Procedure [12-6](#) to enable or disable the PCI function of an eNodeB.

PCI procedures

Perform the following procedures to configure the PCI function of eNodeBs.

Procedure 12-6 To enable or disable PCI on an eNodeB



Note 1 — Enabling the PCI feature on an eNodeB consumes a RAN license feature entitlement token.

Note 2 — ANR must be enabled in order for the PCI function to have an effect on eNodeB neighbor relations.

- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
 - 2 Click on the Components tab button.
 - 3 Navigate to the Activation Service object. The path is eNodeB NE Instance→Activation Service→Activation Service ID *n*.
 - 4 Right-click on the Activation Service ID *n* object and choose Properties from the contextual menu. The Activation Service (Edit) form opens.
 - 5 Configure the isSonPciAllocationEnabled parameter to enable or disable PCI on the eNodeB.
 - 6 Click on the OK button to close the form and return to the eNodeB NE Instance form.
 - 7 Click on the Apply button. A confirmation form appears.
 - 8 Click on the Yes button to confirm the changes and close the confirmation form. The changes to the Activation Service object are saved and RAN license token consumption is updated.
 - 9 Close the eNodeB NE Instance form.
-

Procedure 12-7 To configure PCI on an eNodeB

Perform this procedure to do the following:

- Enable or disable PCI conflict correction and configure timer for automatic PCI resolution
 - Add or remove entries in the PCI allowed list
- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
 - 2 Click on the Components tab button.

- 3 Navigate to the Automatic Physical Cell Identify object. The path is eNodeB NE Instance→Self Organizing Network→Automatic Physical Cell Identity→Automatic Physical Cell Identity ID *n*.
- 4 Right-click on the Automatic Physical Cell Identity ID *n* object and choose Properties from the contextual menu. The Automatic Physical Cell Identity (Edit) form opens with the General tab displayed.
- 5 Configure PCI conflict correction, as required:
 - i Configure the enableMaintenancePeriod parameter to enable or disable automatic PCI conflict correction.
 - ii Configure the maintenancePeriodStartTime (h) parameter to specify the time, in hours, that the eNodeB will wait before activating automatic PCI conflict correction function.
- 6 Configure the PCI allowed list, as required:



Note 1 – Values in the PCI allowed list define a list of PCI values that can be used by eNodeB cells. If the list is empty, all 504 possible values are available to the eNodeB.

Note 2 – You can delete a value from the PCI allowed list by choosing the value from the list and clicking on the Delete button.

- i Click on the Pci Allowed List tab button.
 - ii Click on the Add button. The Entry form opens.
 - iii Configure the Value parameter with an integer ranging from 0 to 503.
 - iv Click on the OK button to close the Entry form and add the PCI value to the list.
 - v Repeat the previous two steps to add more PCI values to the list, as required.
 - vi Click on the OK button to close the Automatic Physical Cell Identity (Edit) form.
- 7 Click on the Apply button. A confirmation window opens.
- 8 Confirm the changes and close the eNodeB NE Instance form.

LTE RAN maintenance

13 – LTE RAN device maintenance

14 – LTE RAN statistics

15 – LTE RAN troubleshooting

13 – LTE RAN device maintenance

13.1 Overview	13-2
13.2 Workflow to manage LTE RAN maintenance	13-2
13.3 NE maintenance preparation	13-2
13.4 eNodeB backup and restore	13-4
13.5 eNodeB software upgrades	13-11

13.1 Overview

The 5620 SAM includes NE maintenance functionality for supported RAN devices that allows a system administrator to:

- perform an on-demand or scheduled NE configuration backup
- perform an on-demand or scheduled eNodeB software upgrade
- view the status of a deployment, backup, or device software upgrade
- troubleshoot a failed deployment, backup, or upgrade
- support hardware maintenance activities

A 5620 SAM operator with an administrator or network element software management scope of command role can perform device configuration save, backup, or restore operations and can create policies for scheduling backups. See the *5620 SAM User Guide* for more information about the backup and restore and software upgrade functionality of the 5620 SAM.

See the *5620 SAM Maintenance Guide* for information about recurring maintenance tasks that can be performed on the 5620 SAM server system.

13.2 Workflow to manage LTE RAN maintenance

- 1 Perform backup and restore operations for eNodeBs, as required.
 - i Create RAN backup policies and assign them to eNodeBs. See Procedure [13-2](#).
 - ii Configure the 5620 SAM to save eNodeB backups to the 5620 SAM main server file system, if required. See Procedure [13-4](#).
 - iii Perform immediate eNodeBs backups, as required. See Procedure [13-5](#).
 - iv Restore eNodeB device configurations, as required. See Procedure [13-6](#).
- 2 Perform eNodeBs software upgrade operations, as required.
 - i Create and assign eNodeB software upgrade policies. See Procedure [13-7](#).
 - ii Import eNodeB software images to the 5620 SAM. See Procedure [13-8](#).
 - iii Perform immediate eNodeBs software upgrades, as required. See Procedure [13-9](#).
 - iv Monitor the software upgrade status. See Procedure [13-10](#).

13.3 NE maintenance preparation

You must ensure that preparation tasks are completed prior to using the 5620 SAM to perform maintenance operations such as device configuration backup and device software upgrade.

Network preparation

Preconfiguration of user accounts and system settings is a requirement for LTE RAN device maintenance tasks.

User accounts

FTP and SFTP transfers between eNodeBs and the 5620 SAM require the preconfiguration of user accounts. You can use the samadmin user for FTP and SFTP transfers, or create a specialized account.

Software upgrades

LTE RAN device software upgrades are best performed as a multi-step process over a period of days or weeks. The following conditions and considerations for device software upgrades are presented as an example to aid network administrators in upgrade planning. Contact Alcatel-Lucent Customer Support before performing a software upgrade on LTE RAN devices.

Software upgrade conditions

Verify that the following conditions are true to help ensure the success of a device software upgrade.

- Login accounts are prepared for the 5620 SAM.
- Devices selected for software upgrade are managed by the 5620 SAM.
- Device downtime of several minutes is accommodated by the network plan.
- Deltas between existing parameter configurations and new parameter defaults are known and planned for.
- 9952 WPS considerations such as current 9952 WPS version and WO creation are taken into account.

Performing the software upgrade

Verify that the following conditions are true before proceeding with the software upgrade.

- Call trace sessions are not running on devices.
- Release notices and bulletins are understood by network administration.
- Software image downloads to target devices are complete.
- No critical alarms are affecting LTE RAN or ePC devices.
- No hardware configurations or feature activations are being carried out on LTE RAN or ePC devices.
- RAN licensing capacity is sufficient to accommodate the upgrade.
- WOs for newly upgrades devices are ready for deployment.
- Alcatel-Lucent Customer Support contact information is known to operators.

Network preparation procedures

Perform the following procedures to help prepare the 5620 SAM network for RAN devices.

Procedure 13-1 To assign a password to the samadmin user

The 5620 SAM installer creates a user account called samadmin that is required for 5620 SAM system administration. FTP and SFTP transfers between the 5620 SAM and the eNodeB require a password to be set for the samadmin user.



Caution 1 — Do not use the @ character in the samadmin user password. Backup file transfers will fail if the samadmin user password contains the @ character.

Caution 2 — Alcatel-Lucent strongly recommends that strict password controls are exercised for the samadmin user.



Note — Perform this procedure only if a password has not been set for the samadmin user during the 5620 SAM installation process, or if the samadmin user password contains a restricted character that impacts eNodeB operation.

1 Log in to the 5620 SAM server as the root user and open a console window.

2 Enter the following at the CLI prompt:

```
# passwd samadmin
```

The following prompt is displayed:

```
New Password:
```

3 Enter the new password and press ↵.

The following prompt is displayed:

```
Re-enter new password:
```

4 Enter the new password again and press ↵. The following message is displayed:

```
passwd: password successfully changed for samadmin
```

5 Close the console window.

13.4 eNodeB backup and restore

The 5620 SAM provides a function to backup and restore eNodeB SNMP MIB parameters only. The SNMP parameters included in eNodeB backup files are the alpha and beta transport parameters for OAM communication and hardware configuration. The gamma parameters of the eNodeB NetConf MIM are not included in eNodeB backup files.

You must perform eNodeB NE backup and restore in conjunction with configuration snapshots and WO deployment in order to capture and be able to restore the full eNodeB NE configuration. Device backups and configuration snapshots can both be configured to occur on a recurring schedule in order to provide fully automatic backup capability for the eNodeB.



Note — The Save Config (configuration save) function of the 5620 SAM is not supported for the eNodeB and the command performs no action on the device.

A default RAN-based backup and restore policy is created when the 5620 SAM is installed. The backup policy that is assigned to a device is determined by the discovery rule. See chapter 5 for more information about configuring discovery rules.

The following steps describe the recommended process for eNodeB NE backup:

- 1 Configure an eNodeB backup and restore policy, or use the default RAN-based backup and restore policy.
- 2 Assign a backup and restore policy to eNodeBs, as required.
- 3 Schedule recurring configuration snapshots to coincide with the scheduled backup interval specified by the assigned RAN-based backup and restore policy. See chapter 6 for more information about configuration snapshots.

The following steps describe the recommended process for eNodeB NE restore:

- 1 Use the 9952 WPS to convert a configuration snapshot taken by the 5620 SAM into a WO.
- 2 Perform Procedure 13-5 to restore the most recent backup, or perform Procedure 13-6 to restore a backup other than the most recent.
- 3 Perform Procedures 6-1 and 6-2 to use the activation manager to deploy the WO described in step 1 to the eNodeB. See chapter 6 for more information about using the activation manager.

The 5620 SAM holds and automatically purges device backup files according to the applicable backup policy. You can schedule configuration restores or perform them immediately.



Note 1 — You cannot restore a RAN device configuration that uses an outdated software version after performing a software upgrade on the device.

Note 2 — The Administrative State of an eNodeB is set to Locked after a successful restore operation. Perform Procedure 7-4 to unlock an eNodeB.

Backup and restore procedures

Perform the following procedures to configure and perform the backup and restore function of the 5620 SAM for the eNodeB. See the *5620 SAM Parameter Guide* for descriptions of the parameters in the following procedures.

Procedure 13-2 To create or modify a RAN backup/restore policy

- 1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.
- 2 Perform one of the following.
 - a Create a RAN backup/restore policy.
 - i Click on the Create button. The Backup Policy (Create) form opens.
 - ii Configure the parameters:
 - Auto-Assign ID
 - Policy ID
 - iii Enter a name for the backup policy in the Name field.
 - iv Choose eNodeB from the Policy Type drop-down menu. The form refreshes to display eNodeB-specific parameters. Go to step 3.
 - b Modify a RAN backup policy.
 - i Configure the filter criteria, if required, and click on the Search button. A list of backup policies is displayed.
 - ii Choose a backup policy from the list that displays eNodeB Node as its Policy Type and click on the OK button. The Backup Policy (Edit) form opens with the General tab displayed. Go to step 3.
- 3 Specify whether backup functionality is enabled.
 - a Select the Enable Backup check box.
 - b Deselect the Enable Backup check box. Go to step 7.
- 4 In the Backup Triggering panel, configure the parameters:
 - Scheduled Backup Scheme
 - Scheduled Backup Interval
 - Scheduled Backup Sync Time
 - Scheduled Backup Threshold (operations)
 - Auto Backup Threshold (operations)
- 5 In the Backup Purging panel, configure the parameters:
 - Auto Purge Scheme
 - Number Of Backups
 - Maximum Backup Age (days)

6 In the eNodeB Backup Settings panel, configure the following parameters:

- SFTP/FTP User ID
- SFTP/FTP Password



Note 1 — You must enter the samadmin user as the SFTP/FTP User ID and the samadmin user password as the SFTP/FTP Password.

Note 2 — Backup file transfers from the eNodeB to the 5620 SAM will fail if the samadmin password contains the @ character. Perform Procedure 13-1 to set a new password for the samadmin user.

Note 3 — The Root Directory parameter (read-only) specifies a temporary location for the device backup files. Perform Procedure 13-4 to specify an additional location for device backup files on the 5620 SAM server.

7 Perform one of the following:

- a If you are creating a new backup policy and need to assign the policy to eNodeBs, click on the Apply button. The Backup Policy (Create) form refreshes with additional tabs and the name of the form changes to Backup Policy (Edit). Go to step 8.
- b If you are creating a new backup policy and do not need to assign it immediately:
 - i Click on the OK button to save the backup policy and close the form.
 - ii When you need to assign the backup policy, perform this procedure to modify the backup policy, if required, and assign the policy to eNodeBs.
- c If you are modifying an existing backup policy, go to step 8.

8 Click on the Backup/Restore Policy Assignment tab button. The Backup Policy Filter opens.

9 Configure the filter criteria, if required, and click on the OK button to close the Backup Policy Filter form.

10 Using the right and left arrows in the center of the form, move eNodeBs between the Unassigned Sites panel and the Assigned Sites panel as required.

11 Click on the Apply button. A confirmation dialog appears.

12 Click on the Yes button to confirm the action, assign the backup policy to the selected eNodeBs, and close the dialog.

13 Perform one of the following.

- a Close the Backup/Restore form.
- b Monitor backup and restore status as required. See the *5620 SAM User Guide* for more information on the backup and restore functionality of the 5620 SAM.

Procedure 13-3 To delete a backup/restore policy

Perform this procedure to delete a custom backup/restore policy.



Note 1 — You cannot delete a default backup/restore policy.

Note 2 — You cannot delete a policy if it is currently assigned to a device.

- 1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.
 - 2 Choose a backup/restore policy from the list and click on the Delete button. A confirm form opens.
 - 3 Click on the Yes button. The backup/restore policy is deleted.
 - 4 Close the Backup/Restore form.
-

Procedure 13-4 To configure the 5620 SAM to save RAN device configuration backups on a file system

Perform this procedure to configure the 5620 SAM to save RAN device configuration backups as files in addition to saving them to the specified FTP/SFTP server.



Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.



Note 1 — The samadmin user requires read and write permissions to each directory specified in this procedure.

Note 2 — The Solaris command lines in this procedure use the # symbol to represent the command prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

- 1 Log in to the 5620 SAM server station as the samadmin user.
- 2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.
- 3 Create a backup copy of the nms-server.xml file.
- 4 Open the nms-server.xml file using a plain-text editor.
- 5 Search for the following XML tag:

`<RanBackup`
- 6 Enable file-system storage for backups of RAN devices by modifying the following line:


```
RanBackupDirectory="path"
```

where *path* is an absolute or relative file path



Note — A relative file path that you specify in this step is relative to the *installation_directory/nms/bin* directory on the 5620 SAM server.

- 7 Save and close the nms-server.xml file.
- 8 Navigate to the 5620 SAM server binary directory, typically */opt/5620sam/server/nms/bin*.
- 9 Enter the following command at the prompt:

```
# ./nmsserver.bash read_config .
```

The 5620 SAM main server reads the nms-server.xml file and puts the configuration change into effect. Subsequent RAN device configuration backups are saved to the path specified in the nms-server.xml file.

Procedure 13-5 To perform an immediate eNodeB backup or restore

When you start an immediate backup, you back up the device configuration based on the backup policy associated with the eNodeB. An eNodeB configuration restore operation uses the most recently backed-up eNodeB configuration file unless otherwise specified. See Procedure 13-6 for more information about restoring a device configuration that is not the most recent.



Note — The Administrative State of an eNodeB is set to Locked after a successful restore operation. Perform Procedure 7-4 to unlock an eNodeB.

The following conditions must be present before you can perform a device configuration backup, restore, or configuration save:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See the *5620 SAM User Guide* for more information.
- FTP or SFTP is configured in the mediation policy for the eNodeB. See chapter 5 for more information.

Depending on the operation type, the Backup State or Restore State column displays the current state of the operation. The possible values are:

- Not Attempted - the operation is unattempted
- Saving Config - the device configuration is being saved on the device
- Transferring files - a file transfer is in progress

- Success - the operation is complete and successful
- Failure - the operation is complete but unsuccessful



Note — During a backup, if a device is unresponsive to the 5620 SAM because SNMP on the device is disabled, the Backup State column entry for the device does not immediately display the correct value of Failed. This latency is caused by the inability of the 5620 SAM to communicate with the unresponsive device. In such a situation, the Backup State column displays the initial value of Saving Config until three 10-minute SNMP polling periods, or 30 minutes, have elapsed, after which the Backup State changes to Failed if SNMP remains disabled.

- 1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.
 - 2 Click on the Backup/Restore Status tab button. The managed devices are listed.
 - 3 Select an eNodeB from the list and perform one of the following steps, depending on the operation that you want to perform.
 - a Click on the Backup button.
 - b Click on the Restore button.A confirm form opens.
 - 4 Click on the Yes button. The backup or restore operation starts, and the current backup or restore state for the device is indicated in the Backup State or Restore State column.
 - 5 You can resynchronize an NE with the 5620 SAM database, if required, by clicking on the Resync button. See the *5620 SAM User Guide* for more information about resynchronizing NEs.
 - 6 Close the Backup/Restore form.
-

Procedure 13-6 To restore a device configuration backup other than the most recent

You can choose to restore an older version of the eNodeB configuration to meet special network requirements.



Caution 1 — Older backups do not have the most recent network information. Restoring an older device configuration may be service-affecting.

Caution 2 — Ensure that you back up the current device configuration using Procedure 13-2 before you proceed.

- 1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.
 - 2 Click on the Backup/Restore Status tab. The managed devices are listed.
 - 3 Double-click on a device from the list. The NE Backup/Restore Status form for the selected device opens.
 - 4 Click on the Backups tab button. A list of configuration backups for the selected device opens, ordered from the oldest to the most recent.
 - 5 Select a backup in the list and click on the Restore button. A dialog box appears.
 - 6 Click on the Yes button.
 - 7 Click on the Resync button to ensure the latest network information is available, if required.
 - 8 Close the Backup/Restore form.
-

13.5 eNodeB software upgrades

This section describes software maintenance operations and procedures designed specifically for the eNodeB. Software upgrade support for RAN devices uses the existing function of the 5620 SAM for software management. When a new eNodeB software version is available, you can use the 5620 SAM to perform an on-demand eNodeB software upgrade, or schedule one using a software upgrade policy.

Software management of the eNodeB with 5620 SAM requires you to do the following:

- 1 Download software images from the ALED website to a 5620 SAM client station.
- 2 Upload software images to the 5620 SAM server.
- 3 Schedule device software upgrades with a software upgrade policy, or perform device software upgrades manually.
- 4 Monitor software upgrade status.
- 5 Accept or reject software upgrades, as required.

eNodeB software upgrade policies

A default eNodeB software upgrade policy is created when the 5620 SAM is installed. Unless specified in the discovery rules that add eNodeBs to the network, the default eNodeB software upgrade policy is assigned to all eNodeBs upon discovery by the 5620 SAM. You cannot delete a software upgrade policy that is assigned to an eNodeB. You cannot perform an in-service software upgrade for an eNodeB. An eNodeB software upgrade policy includes the following information:

- SFTP credentials
- software version fallback timers
- automatic software activation and acceptance settings

eNodeB software images

LTE RAN device software images are available at the ALED website. You can access the ALED website at the following address:

`https://download.support.alcatel-lucent.com`

Software images are downloaded as .gz files that must be uncompressed on a client station before being uploaded to the 5620 SAM server. It is recommended that you create a new directory for the extracted files. The following directories and subdirectories are created when you uncompress the files:

- *path/DELIVERY/ENODEB/eNodeB software image identifier*
- *path/DESCRIPTION/ENODEB*

where

path is the directory where you uncompressed the .gz file

eNodeB software image identifier is the version designation of the software image, such as ENBLA0200D60E06601

The DELIVERY directory and subdirectories contain the software image data that is transferred to the 5620 SAM server. The DESCRIPTION/ENODEB directory contains an XML description file. The description file is the file that you must select for import to the 5620 SAM server in Procedure 13-8. The contents of the DELIVERY/ENODEB directory are automatically uploaded to the 5620 SAM server and stored in the database when you import the description file. Therefore, you must maintain the relative directory structure of the uncompressed software image files on your client station for the software image upload to be successful.

The 5620 SAM copies eNodeB software images from the 5620 SAM database to the server file system when a download operation to the NE is initiated. Software images are stored in *installation_directory/lte/enodeBSoftwareRepository*, where *installation_directory* is the 5620 SAM installation location, typically */opt/5620sam*.



Warning — Do not make manual modifications to the *installation_directory/lte/enodeBSoftwareRepository* directory, including manually deleting images, uploading images, and creating subdirectories. Manual modifications to the directory can cause errors when downloading software images to NEs.

Perform Procedure 13-8 to upload an eNodeB software image to the 5620 SAM server. Perform Procedure 13-11 to delete an eNodeB software image from the 5620 SAM server.

eNodeB software upgrade procedures

You can use the 5620 SAM to perform an immediate NE software upgrade or schedule one using a software upgrade policy. You can create and configure multiple eNodeB software upgrade policies and assign them to multiple eNodeBs.

See the *5620 SAM User Guide* for more information about the software upgrade function of the 5620 SAM. See the *5620 SAM Parameter Guide* for descriptions of the parameters in the following procedures.

Procedure 13-7 To create an eNodeB software upgrade policy

- 1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.
- 2 Perform one of the following.
 - a Create a software upgrade policy.
 - i Click on the Create button. The Software Upgrade Policy (Create) form opens.
 - ii Configure the parameters:
 - Policy ID
 - Auto-Assign ID
 - iii Choose eNodeB Node from the Policy Type drop-down list. The eNodeB Based Setting panel appears at the bottom of the form. Go to step 3.
 - b Modify an existing software upgrade policy.
 - i Configure the filter criteria, if required, and click on the Search button. A list of software upgrade policies is displayed.
 - ii Choose a software upgrade policy from the list and click on the Properties button. The Software Upgrade Policy (Edit) form opens with the General tab displayed.
 - iii Go to step 3.

3 Configure the parameters:

- Name
- SFTP User ID
- SFTP Password
- Auto-Activate After Successful File Transfer
- SFTP Server Port
- Timer to Wait for Fallback to Previous Software Version (min)
- Auto-Accept After Successful Software Activation



Note — The samadmin user and password must be used for SFTP User ID and SFTP Password.

4 Perform one of the following:

- a If you are creating a new software upgrade policy and need to assign the policy to eNodeBs, click on the Apply button. The Software Upgrade Policy (Create) form refreshes with additional tabs and the name of the form changes to Software Upgrade Policy (Edit). Go to step 5.
- b If you are creating a new software upgrade policy and do not need to assign it immediately:
 - i Click on the OK button to save the software upgrade policy and close the form.
 - ii When you need to assign the software upgrade policy, perform this procedure to modify the policy, if required, and assign the policy to eNodeBs.
- c If you are modifying an existing software upgrade policy and need to assign the policy to eNodeBs, go to step 5.

5 Assign the software upgrade policy as required.

- i Click on the Software Upgrade Policy Assignment tab button. The Software Upgrade Policy Filter form opens.
- ii Configure the filter settings and click on the OK button to apply the filter. Applying a blank filter brings up a list of all discovered devices.



Note — Alcatel-Lucent does not recommend assigning an eNodeB software upgrade policy to non-RAN devices.

- iii Using the right and left arrows in the center of the form, move eNodeBs between the Unassigned eNodeB panel and the Assigned eNodeB panel as required.
- iv Click on the Apply button and acknowledge the message in the dialog box to assign the software upgrade policy to the devices listed in the Assigned Sites panel.

- 6 Close the Software Upgrade Policy (Edit) form.
 - 7 Close the Software Upgrade form.
-

Procedure 13-8 To import an eNodeB software image into the 5620 SAM

This procedure assumes that you have downloaded and uncompressed an eNodeB software image .gz file to a known directory on a single-user client or client delegate server station, and are aware of the location of the XML description file.



Note 1 — You must preserve the directory structure of extracted software image files.

Note 2 — The samadmin user must have file permissions for software images stored on the 5620 SAM delegate server.

Software images uploaded to the 5620 SAM server are stored in the database.

- 1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.
- 2 Click on the Software Images tab button.
- 3 Click on the eNodeB Software Images tab button.
- 4 Click on the Import button. The Select eNodeB Import Description File window opens.
- 5 Navigate to the DESCRIPTION/ENODEB directory that contains the appropriate software image description XML file.
- 6 Choose the description file and click on the Open button.

The software image appears in the list with In Progress displayed in the Storing Image in DB column. The upload is complete when the status in this column displays as Done.

Procedure 13-9 To perform an immediate software upgrade on an eNodeB



Danger — LA/TLA2.x eNodeBs do not support locking when the software upgrade status is Activated (the software is not yet Accepted). When you attempt to lock LA/TLA2.x eNodeBs that have a software upgrade status of Activated, the following events occur:

- The 5620 SAM raises a deployment failure alarm. The alarm states that the BS Communication State is “Offline”. The Current Operational State parameter continues to display “Enabled”.
- The Administrative State parameter displays “Locking in Progress” in the ENB Equipment properties form of the eNodeB. The eNodeB remains online and transmitting.
- The Administrative State parameter continues to display “Locking In Progress” until the software upgrade is Accepted, and the deployer or an operator successfully retries the lock request.

This issue does not affect eNodeB version LA/TLA3.x or higher. See Procedure 7-4 for more information about locking eNodeBs.

The following conditions must be true before you attempt an eNodeB software upgrade:

- You must have a 5620 SAM user account with an administrator or network element software management scope of command role, or a scope of command role with write access to the mediation package.
 - FTP or SFTP is configured in the mediation policy for the device. See chapter 5 for more information.
- 1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.
 - 2 Click on the Software Images tab button. The form refreshes with additional tabs.
 - 3 Click on the eNodeB Software Images tab button.
 - 4 Transfer software images from the 5620 SAM to the selected eNodeBs.
 - i Click on the Download Image button. The Select Sites form opens.
 - ii Choose one or more eNodeBs from the list and click on the OK button to begin the transfer and close the form.



Note — The 5620 SAM monitors download progress automatically. If SNMP traps from the eNodeB are not being sent and download status does not update, click on the Check Download Progress button to force a check.

- 5 Schedule image downloads, if required.
 - i Click on the Schedule Download Image button. The SAM Schedule (Create) form opens with the General tab displayed.
 - ii Configure the scheduling information. See the *5620 SAM User Guide* for more information on using the 5620 SAM scheduler.

- 6 Abort image downloads by clicking on the Abort Image Download button, as required.
- 7 Delete images by clicking on the Delete button, as required.
- 8 Activate software images and monitor activation progress.
 - i Click on the Activate Image button. The Select Sites form opens.
 - ii Choose one or more eNodeBs from the list and click on the OK button to activate the image and close the form.
- 9 Accept the software image and finalize the software upgrade, as required.
 - i Click on the Accept Image button. The Select Sites form opens.
 - ii Choose one or more eNodeBs from the list and click on the OK button to accept the image and close the form.
- 10 Reject the software image and reverse the software upgrade, if required.



Note — Rejecting a software image effectively performs a software downgrade on the eNodeB, forcing it to revert to the previous software version.

- i Click on the Reject Image button. The Select Sites form opens.
 - ii Choose one or more eNodeBs from the list and click on the OK button to reject the image and close the form.
-

Procedure 13-10 To monitor software upgrade status

- 1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.
- 2 Click on the Software Upgrade Status tab button.
- 3 Click on the eNodeB Upgrade Status tab button.
- 4 Configure the filter criteria, if required, and click on the Search button. A list of eNodeBs is displayed.
- 5 Perform the following steps, as required.
 - a Activate software images by clicking on the Activate button.
 - b Accept software upgrades by clicking on the Accept button.
 - c Reject software upgrades and revert to the previously installed software version by clicking on the Reject button.

- d Reload software images by clicking on the Reload button.
 - e Abort software upgrades that are in progress by clicking on the Abort button.
-

Procedure 13-11 To delete an eNodeB software image from the 5620 SAM server

- 1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.
 - 2 Click on the Software Images tab button.
 - 3 Click on the eNodeB Software Images tab button.
 - 4 Choose an eNodeB software image from the list and click on the Delete button.
 - 5 Close the Software Upgrade form.
-

14 – LTE RAN statistics

- 14.1 Overview 14-2**
- 14.2 Workflow to manage LTE RAN statistics 14-2**
- 14.3 eNodeB PM statistics 14-2**
- 14.4 LTE statistics configuration 14-7**
- 14.5 PCMD 14-10**
- 14.6 eNodeB radio measurement 14-11**

14.1 Overview

This chapter describes the process for configuring eNodeB-specific statistics functions of the 5620 SAM. PM statistics are collected at regular, configurable intervals from eNodeBs by the 5620 SAM server in the form of compressed files that can be transferred via FTP. Retrieval of individual PM counters from the eNodeB via OSS interface is not supported.

You can view eNodeB PM statistics using the 9959 NPO. Plotting eNodeB statistics using the 5620 SAM statistics plotting function is not supported.

See Appendix A for a listing of eNodeB PM statistics counters by 3GPP name. See the *Alcatel-Lucent 9412 eNodeB Counters Reference Guide 418-000-035* for descriptive information about eNodeB PM statistics counters.

14.2 Workflow to manage LTE RAN statistics

- 1 Configure statistics data synchronization for a redundant 5620 SAM deployment, if required, during system installation or reconfiguration. See “[LTE PM statistics synchronization](#)” for more information.
- 2 Create or modify RAN performance management policies, assign eNodeBs to the policies, and enable the policies. See Procedure [14-1](#).
- 3 Configure the maximum SNMP block size for PM statistics transfers to the 5620 SAM, if required. See Procedure [14-2](#).
- 4 Configure the PM statistics counter group selection, if required. See Procedure [14-3](#).
- 5 Configure PM statistics synchronization, as required. See Procedure [14-4](#).
- 6 Configure PCMD for eNodeBs, as required. See Procedure [14-5](#).
- 7 View eNodeB radio measurements. See Procedure [14-6](#).

14.3 eNodeB PM statistics

This section describes the collection of eNodeB PM statistics by the 5620 SAM.

Statistics collection overview

The eNodeB automatically starts recording PM statistics when commissioned and continues recording the statistics indefinitely. The eNodeB collects statistics by storing counters in its memory and writing the counters to a file approximately 30 s after the end of the defined collection interval, depending on network traffic levels.

The recorded statistics file is compressed and mediated to the SNMP interface of the eNodeB. The 5620 SAM retrieves the statistics file from the eNodeB via SNMP at the end of the collection interval that is defined in the RAN performance management policy. The 5620 SAM retains eNodeB PM statistics files in the server file system for the time period that is specified in the nms-server.xml file. The 5620 SAM does not read eNodeB PM statistics files or add counter values to the database.

All discovered and pre-provisioned eNodeBs are added to the default RAN performance management policy, which has an Administrative State of Down and cannot be modified. You must create a new RAN performance management policy, assign eNodeBs to the policy, and set the policy Administrative State to Up before you can collect eNodeB PM statistics using the 5620 SAM.



Note 1 – The 5620 SAM and managed eNodeBs must use a common time-synchronization server that runs a protocol such as NTP. The retrieval of eNodeB PM statistics files by the 5620 SAM will fail when the eNodeB and 5620 SAM real-time clocks are not synchronized.

Note 2 – You can configure the block size for SNMP PM statistics file transfers. Alcatel-Lucent recommends setting the block size to 6000 bytes. Perform Procedure 14-2 to set the maximum block size for PM statistics file transfers from an eNodeB to the 5620 SAM.

The default collection interval for statistics files is 15 min. Statistics are collected and sent even when no counter changes are occurring on an eNodeB. Any failure to receive statistics files from an eNodeB with an active performance management policy will cause an alarm in the 5620 SAM.

eNodeB statistics storage on the 5620 SAM server

The eNodeB PM files are stored in the following directory on the 5620 SAM server:

base directory/lte/stats/*date*/eNodeB/*eNodeB name* directory

where

base directory is the 5620 SAM base directory, typically opt/5620sam

date is the date of PM statistics collection

eNodeB name is the name of the eNodeB

An eNodeB PM file name has the following format:

A[YYYYMMDD].[start time][offset]-[end time][offset]_eNodeB-[eNodeB name]

where

YYYYMMDD is the collection date of the first record in the file

start time is the UTC collection start time in the format HHMM and *offset* is the offset from UTC (always +0000)

end time is the UTC collection end time in the format HHMM and *offset* is the offset from UTC (always +0000)

eNodeB name is the name of the eNodeB

PM counter selection

You can select the counter groups that individual eNodeBs report to the 5620 SAM by configuring parameters on the eNodeB Performance Management object, which is a child object of the eNodeB instance. PM counter group selection is supported on eNodeB version LA4.0 and later. See Procedure [14-3](#) for more information about configuring PM counter group selection.

RAN PM statistics procedures

Perform the following procedures to configure the 5620 SAM to collect eNodeB PM statistics. See the *5620 SAM Parameter Guide* for descriptions of the parameters in the following procedures. See the *5620 SAM LTE Parameter Reference* for descriptions of eNodeB device parameters.

Procedure 14-1 To create or modify an eNodeB performance management policy



Note 1 — The default value for the Administrative State parameter for an eNodeB performance management policy, including the default policy, is Down.

Note 2 — You cannot modify the default eNodeB performance management policy. You must create a new eNodeB performance management policy and set the Administrative State to Up in order to collect eNodeB PM statistics using the 5620 SAM.

Note 3 — You cannot unassign an eNodeB from a PM policy. You can assign an eNodeB to a user-defined PM policy, or you can assign an eNodeB to the default PM policy. Assigning an eNodeB to the default policy effectively disables PM statistics collection for the NE.

- 1 Choose Tools→Statistics→RAN Performance Management Policies from the 5620 SAM main menu. The RAN Performance Management Policies form opens.
- 2 Perform one of the following.
 - a Create an eNodeB performance management policy.
 - i Click on the Create button. The eNodeB Performance Management Policy (Create) form opens.
 - ii Configure the parameters:
 - Policy ID
 - Auto-Assign ID
 - iii Click on the Apply button. The eNodeB Performance Management Policy (Create) form refreshes with additional tabs and the name of the form changes to eNodeB Performance Management Policy (Edit).
 - b Modify an eNodeB performance management policy.
 - i Configure the filter criteria, if required, and click on the Search button. A list of eNodeB performance management policies is displayed.
 - ii Choose an eNodeB performance management policy from the list and click on the Properties button. The eNodeB Performance Management Policy (Edit) form opens.
- 3 Configure the parameters:
 - Displayed Name
 - Description
 - Administrative State
 - Collection Interval (min)
- 4 Click on the Apply button. A dialog box appears.
- 5 Click on the Yes button. The changes are saved.

- 6 To assign the policy to one or more eNodeBs:
 - i Click on the eNodeB Elements tab button.
 - ii Configure the filter criteria, if required, and click on the Search button. A list of eNodeBs that are assigned to the RAN performance management policy is displayed.
 - iii Click on the Assign eNodeBs button. The Assign and Assign Filter forms open.
 - iv Configure the filter criteria, if required, and click on the OK button to close the Assign Filter form and return to the Assign form.
 - v Using the right arrow in the center of the form, move eNodeBs from the Unassigned eNodeB panel to the Assigned eNodeB panel, as required.
 - vi Click on the OK button. The Assign form closes and the eNodeB performance management policy is assigned to the specified eNodeBs.
 - 7 Close the eNodeB Performance Management Policy (Edit) form.
-

Procedure 14-2 To set the PM maximum SNMP block size for an eNodeB

Perform this procedure to configure the block size for the transmission of PM statistics files from the eNodeB to the 5620 SAM.



Note 1 — Alcatel-Lucent recommends setting a value of 6000 for the PM Max Result String Block Size (bytes) parameter in order to optimize network performance in the retrieval of PM statistics files from eNodeBs. The 5620 SAM raises a PMCMaXResultStringBlockSizeNotOptimum alarm when the PM Max Result String Block Size (bytes) parameter is set to a value lower than 6000.

Note 2 — The default value of the PMC Max Result String Block Size (bytes) parameter on eNodeBs may be lower than 6000 bytes. Due to this default value, the PMCMaXResultStringBlockSizeNotOptimum alarm may be raised against multiple eNodeBs.

Note 3 — Depending on the network configuration, it may not be possible to set the PM Max Result String Block Size (bytes) parameter to 6000 bytes. You can configure a specific alarm policy to modify the behavior of the PMCMaXResultStringBlockSizeNotOptimum alarm, including squelching the alarm to prevent the 5620 SAM from raising it. See the *5620 SAM User Guide* for more information about setting specific alarm policies.

- 1 Perform Procedure 7-1 to open the ENB Equipment properties form for an eNodeB.
- 2 In the Performance Management panel, enter a value in the PM Max Result String Block Size (bytes) field. The recommended value is 6000.
- 3 Click on the OK button to close the ENBEquipment form.

- 4 Click on the OK button. A dialog box appears.
 - 5 Click on the Yes button to close the dialog box and save the changes.
-

Procedure 14-3 To configure PM statistics counter group selection for an eNodeB

PM statistics counter group select is supported on eNodeB version LA4.0 and later.

- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
 - 2 Click on the Components tab button.
 - 3 Navigate to the Performance Management object. The path is eNodeB NE Instance→Performance Management→Performance Management ID: *n*.
 - 4 Right-click on the Performance Management ID: *n* object and choose Properties from the contextual menu. The Performance Management (Edit) form opens with the General tab displayed.
 - 5 Configure the parameters:

• rrcConnectionReported	• uEContextReported
• uLNoiseReported	• hRPDor1xRTTReported
• mobilityFailureReported	• trafficShaping
• spare1Reported	• specificTDDReported
• rFMeasurementReported	• spare2Reported
• specificTDDERABReported	• geranOrUtranReported
 - 6 Click on the OK button. The Performance Management (Edit) form closes.
 - 7 Click on the Apply button in the eNodeB NE Instance (Edit) form. A dialog box appears.
 - 8 Click on the Yes button. The changes are saved.
 - 9 Close the eNodeB NE Instance (Edit) form.
-

14.4 LTE statistics configuration

This section describes 5620 SAM server functions that facilitate LTE PM statistics management.

LTE PM statistics catch-up

PM statistics catch-up is enabled by default on the 5620 SAM main server. When PM statistics catch-up is enabled, the 5620 SAM retrieves any PM statistics files that have been missed within the time frame specified by the `catchUpInterval` parameter in the `nms-server.xml` file. The default value of `catchUpInterval` is 4320 minutes, or 72 hours. All PM statistics files that exist on eNodeBs and do not exist in the 5620 SAM file system are saved to the file system. Perform Procedure 14-4 to configure PM statistics catch-up.

The 5620 SAM invokes PM statistics catch-up and attempts to retrieve files for the specified time frame under the following conditions:

- the 5620 SAM main server restarts
- an eNodeB reboots
- the 5620 SAM loses and subsequently regains connectivity to an eNodeB

You can manually invoke PM statistics catch-up for specific RAN PM policies over the 5620 SAM-O XML interface using the `Iteperf.RanPMPolicy.invokeCatchup` method. See the *5620 SAM-O XML Reference* for more information about the input parameters of this method. See the *5620 SAM XML OSS Interface Developer Guide* for more information about using the 5620 SAM-O XML interface.

LTE PM statistics synchronization

You can configure a redundant 5620 SAM system to allow replication and synchronization of PM statistics files to the active and standby auxiliary servers. You can enable PM statistics file synchronization during 5620 SAM installation or reconfiguration using the 5620 SAM server configuration utility. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* or contact Alcatel-Lucent technical support for more information.

Statistics configuration procedures

Perform the following procedures to configure statistics collection for LTE devices.

Procedure 14-4 To configure PM statistics catch-up on the 5620 SAM



Caution 1 — Modify only the parameters specified in this procedure. Unauthorized modification of the `nms-server.xml` file can seriously affect network management and 5620 SAM performance.

Caution 2 — This procedure requires a restart of the 5620 SAM main server, which is service-affecting.



Note 1 — PM statistics catch-up is enabled by default. If you disable PM statistics catch-up, in order to enable the function you must perform this procedure, set the enableCatchup parameter to “true”, and restart the 5620 SAM main server.

Note 2 — You do not need to enable the PM catch-up function on 5620 SAM auxiliary servers. Enable PM statistics catch-up on the main servers only.

Note 3 — When using auxiliary servers for PM statistics collection, Alcatel-Lucent recommends setting the deploymentWorker statsPoolSize parameter to 30. See step 6 of this procedure.

- 1 Open a console window and log in to the 5620 SAM main server as the samadmin user.
- 2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.
- 3 Open the nms-server.xml file using a plain-text editor.
- 4 Find the following lines of text in the nms-server.xml file:

```
<statsCatchup
    catchUpInterval="interval_value"
    enableCatchup="enabled_value" />
```

where

enabled_value specifies whether the function is enabled (“true” or “false”).

interval_value specifies the period of time, in mins, for which the 5620 SAM will retrieve missing PM files. The default value is 4320, which equals 72 hours.



Note — You must set the value of the catchUpInterval parameter to an equal or lower value than the value of the timeToKeepFile parameter, as the effective value of the catchUpInterval parameter is limited by the timeToKeepFile parameter.

- 5 Configure the parameters:
 - enabledCatchup
 - catchUpInterval
- 6 Choose one of the following:
 - a If you are configuring PM statistics catch-up on a 5620 SAM installation that does not use auxiliary servers for statistics collection, go to step 7.
 - b If you are configuring PM statistics catch-up on a 5620 SAM installation that uses auxiliary servers for statistics collection, perform the following steps:
 - i Find the following line of text in the nms-server.xml file:

```
<deploymentWorker
```

```
statsPoolSize="value" />
```

where *value* is the number of threads for statistics collection

- ii Set the value of the statsPoolSize parameter to “30”.
- iii Go to step 7.

- 7 Save and close the nms-server.xml file.
- 8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.
- 9 Enter the following at the prompt as the samadmin user:

```
# ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and changes to the file are updated in the 5620 SAM.



Note 1 — If you have disabled and re-enabled PM statistics catch-up, you cannot invoke the lteperf.RanPMPolicy.invokeCatchup method until the 5620 SAM main server is restarted.

Note 2 — If you have modified the statsPoolSize parameter in step 6, you must restart the 5620 SAM main server for the change to take effect.

- 10 Enter the following at the prompt to restart the 5620 SAM main server, if required:

```
# ./nmsserver.bash force_restart ↵
```



Caution — Restarting a 5620 SAM main server is service-affecting. Ensure that you perform this step only during a scheduled maintenance window.

14.5 PCMD

The PCMD function of the eNodeB provides network planners and administrators with call information to aid in network decision-making. You can use the 5620 SAM to enable or disable the PCMD function of the eNodeB. PCMD data can be analyzed using the 9959 NPO.

PCMD procedures

Perform the procedures in this section to manage the PCMD function of the eNodeB.

Procedure 14-5 To enable or disable PCMD on an eNodeB



Note 1 — PCMD is enabled by configuring the isPCMDEnabled parameter on the Subscriber and Equipment Traces object, however, the PCMD function does not require an active call trace.

Note 2 — Enabling PCMD on an eNodeB will consume a feature entitlement token. See chapter 9 for more information.

- 1 Perform one of the following:
 - a Perform Procedure 7-2 to open the eNodeB NE Instance form of an eNodeB.
 - b Perform Procedure 7-5 to use the logical objects manager to open the eNodeB NE Instance form of an eNodeB.
 - 2 Click on the Components tab button.
 - 3 Navigate to a Subscriber And Equipment Traces object. The path is eNodeB NE Instance→Subscriber and Equipment Traces→Subscriber and Equipment Traces ID: *n*.
 - 4 Right-click on the Subscriber and Equipment Traces ID *n* object and choose Properties from the contextual menu. The Subsc and Equipment Traces (Edit) form opens with the General tab displayed.
 - 5 Configure the isPCMDEnabled parameter.
 - 6 Click on the OK button. The Subsc and Equipment Traces (Edit) form closes.
 - 7 Click on the OK button. A dialog box appears.
 - 8 Click on the Yes button. The eNodeB NE Instance form closes.
-

14.6 eNodeB radio measurement

The eNodeB radio measurement function provides operators with the ability to view automatically updated feeds of radio parameter values for a configurable subset of eNodeBs using the 5620 SAM GUI. See Figure 14-1 for an example of the eNodeB Radio Measurement form.

Figure 14-1 eNodeB Radio Measurement form

The screenshot shows a software window titled "eNodeB Radio Measurement (4)". It contains a table with the following columns: Router Id, Cell name, Port number, VSWR, Return loss (dB), RTU Tx Power (dBm), Rx Channel RSSI (dBm), and Timestamp. The table displays six rows of data. To the right of the table, there are controls including a search bar, buttons for "Select eNB", "Refresh", "Properties", and "Copy to Clipboard", and a checkbox for "Auto Refresh (60s)".

Router Id	Cell name	Port number	VSWR	Return loss (dB)	RTU Tx Power (dBm)	Rx Channel RSSI (dBm)	Timestamp
ENB_1064_10_190_6_1	1064_10_190_6_1_0	1	105907211.9	2.5	11.9	377.2	2011.09.09 09:10:53 638 CEST
ENB_1064_10_190_6_1	1064_10_190_6_1_1	1	196526349.6	7.4	5.3	-1551.8	2011.09.09 09:10:53 638 CEST
ENB_1064_10_190_6_1	1064_10_190_6_1_2	1	40004932.1	6.0	9.2	-2061.8	2011.09.09 09:10:53 639 CEST
ENB_1064_10_190_6_1	1064_10_190_6_1_0	2	81856794.1	13.2	17.9	2902.0	2011.09.09 09:10:53 639 CEST
ENB_1064_10_190_6_1	1064_10_190_6_1_1	2	77356068.8	8.5	24.1	-660.4	2011.09.09 09:10:53 640 CEST
ENB_1064_10_190_6_1	1064_10_190_6_1_2	2	6235944.0	7.4	45.1	452.9	2011.09.09 09:10:53 640 CEST

Table 14-1 describes the radio measurement parameters that you can display on-demand in the eNodeB Radio Measurement form.

Table 14-1 Radio measurement parameters

Parameter name	Calculation	Description
VSWR	$(1 + \sqrt{\text{reverse power} / \text{forward power}}) / (1 - \sqrt{\text{reverse power} / \text{forward power}})$	Radio transmission efficiency measured at the antenna port of the RFM. The value is a fixed-comma number with an accuracy of 0.1, encoded as an integer value: 1 = 0.1. Example: A VSWR of 1.5 is encoded as 15. As a ratio it has no physical unit. Special values: -1 = No measurement has been performed. -2 = Internal measurement error.
Return loss (dB)	$-20 * \log((\text{vswrMeasuredValue} - 1) / (\text{vswrMeasuredValue} + 1))$	Signal return loss calculated based on the VSWR measured value per RTU transmission port. Special values: -1 = No measurement has been performed. -2 = Internal measurement error.
RTU Tx Power (dBm)	—	The RTU transmission power per transmitting antenna port. Special values: -1 = No measurement has been performed. -2 = Internal measurement error.
Rx Channel RSSI (dBm)	—	Received radio signal strength. Special values: -32767 = No measurement has been performed. -32768 = Internal measurement error.

Radio measurement is inactive by default on eNodeBs. The 5620 SAM sends a command that activates the radio measurement function on the NE when you select eNodeBs for radio measurement. The eNodeB updates the radio parameters in the device MIM every 60 seconds for a period of 30 minutes when the function is active.



Note 1 – Radio measurement is supported for eNodeB version LA4.1.

Note 2 – Radio parameters that are not applicable to the device object being measured display a value of N/A.

Note 3 – Changes to the radio measurement parameters listed in Table 14-1 do not increment the eNodeB last-change counter.

You can update radio measurement values 5620 SAM GUI using the following methods:

- on-demand by clicking on the Refresh button
- automatically by enabling the Auto Refresh (60s) parameter

On-demand refresh updates the radio parameter values when you click the Refresh button. Auto-refresh updates the radio parameter values every 60 seconds for a period of 30 minutes, which is the same time frame as the NE. Auto-refresh is automatically disabled at the end of the 30-minute time span. You can manually disable auto-refresh by disabling the check box.

You can view the most recently collected radio parameter values for all managed eNodeBs by clicking on the Search button. Clicking on the Search button does not refresh the data.

Radio measurement procedures

Perform the procedures in this section to management eNodeB radio measurement.

Procedure 14-6 To view eNodeB radio measurement using the 5620 SAM GUI

- 1 Choose Tools→Statistics→eNodeB Radio Measurement from the 5620 SAM main menu. The eNodeB Radio Measurement form opens.
- 2 Click on the Select eNB button. The Select Sites list form opens.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of eNodeBs is displayed.
- 4 Select one or more eNodeBs from the list. To select multiple eNodeBs, hold down the CTRL key and click.
- 5 Click on the OK button. The Select Sites list form closes and the updated radio parameter values of the cells and ports of the selected eNodeBs are displayed in the eNodeB Radio Measurement form.

- 6 Verify the following information, as required:
 - VSWR
 - Return loss (dB)
 - RTU Tx Power (dBm)
 - Rx Channel RSSI (dBm)
- 7 To manually refresh the data, click on the Refresh button.
- 8 To enable or disable auto-refresh, select or deselect the Auto Refresh (60s) parameter.



Note — Auto-refresh runs for a time span of 30 minutes. The Auto Refresh (60s) parameter automatically becomes deselected when the time expires.

- 9 To view a specific radio measurement entry, perform the following steps:
 - i Select an entry from the list and click on the Properties button. The eNodeB Radio Measurement - *object_type* (View) form opens with the General tab displayed.
 - ii Verify the following information, as required:
 - Assigned RFM
 - Polling status



Note — The Polling Status parameter specifies whether auto-refresh is running.

- iii Close the eNodeB Radio Measurement - *object_type* (View) form.
 - 10 To redisplay the most recently collected measurement data, click on the Search button.
 - 11 Close the eNodeB Radio Measurement form.
-

15 – LTE RAN troubleshooting

15.1 Overview	15-2
15.2 Workflow to manage LTE RAN troubleshooting	15-2
15.3 Alarms and fault management	15-3
15.4 Event logging	15-7
15.5 Device configuration and database troubleshooting	15-9
15.6 Call trace	15-12

15.1 Overview

The 5620 SAM provides troubleshooting support that is specific to the eNodeB. You can use the 5620 SAM to perform the following troubleshooting tasks for eNodeBs:

- View, acknowledge, and clear eNodeB alarms.
- View the events log for an eNodeB.
- Detect and fix eNodeB configuration errors.
- Troubleshoot network traffic problems using the call trace function.

15.2 Workflow to manage LTE RAN troubleshooting

- 1 Reset eNodeB components to resolve fault conditions, as required. See the following for more information:
 - to perform a full reset on an eNodeB, see Procedure [15-1](#)
 - to reset a base band card or control board card, see Procedure [15-2](#)
 - to reset a RRH, see Procedure [15-3](#)
 - to reset a TRDU, see Procedure [15-4](#)
- 2 Manage event logging for eNodeBs, as required.
 - i View the events log for an eNodeB. See Procedure [15-7](#).
 - ii Configure the event logging policy for an eNodeB. See Procedure [15-8](#).
 - iii Purge the statistics records for an eNodeB. See Procedure [15-9](#).
- 3 Perform eNodeB database reconfiguration and resynchronization operations, as required.
 - i Reconfigure the database of an eNodeB with the NE configuration data that exists in the 5620 SAM database. See Procedure [15-10](#).
 - ii Resynchronize the database of an eNodeB with the 5620 SAM to accept the NE configuration and replace the NE configuration data in the 5620 SAM database. See Procedure [15-11](#).
- 4 Configure call trace for eNodeBs, as required.
 - i Configure global call trace in the 5620 SAM. See Procedure [15-12](#).
 - ii Configure local call trace on eNodeBs. See Procedure [15-13](#).
 - iii Create call trace sessions using the global call trace management form. See Procedure [15-14](#).
 - iv Create call trace sessions using an eNodeB NE instance properties form. See Procedure [15-15](#).
 - v Activate call trace sessions. See Procedure [15-16](#).
 - vi Deactivate call trace sessions. See Procedure [15-17](#).
 - vii Delete call trace sessions. See Procedure [15-18](#).

- viii Create scheduled tasks for the execution of call trace sessions. See Procedure [15-19](#).
- ix Control call trace scheduled task execution. See Procedure [15-20](#).
- x Manage the assignment of eNodeBs to call trace auxiliary-server pairs. See Procedure [15-21](#).

15.3 Alarms and fault management

Alarms represent device and network faults. The 5620 SAM displays incoming alarms from NEs and raises alarms when specific conditions arise in the 5620 SAM network. Alarms that are raised as a result of SNMP traps from eNodeBs are named with an InfoKey number that uniquely identifies the alarm, such as IK4305035.

See the *5620 SAM Troubleshooting Guide* for information about acknowledging, clearing, and correlating alarms using the 5620 SAM. See the *5620 SAM User Guide* for information about configuring alarm policies, alarm behaviors, and general information about using the alarm window. See the *5620 SAM Alarm Reference* for a list of alarms that the 5620 SAM can raise for the eNodeB.

Fault clearance procedures

Fault clearance procedures for eNodeB alarms vary. Perform the procedures in this section when instructed by the Remedial Actions section of an alarm description, or when advised to do so by Alcatel-Lucent technical support. Resetting an eNodeB can clear some fault conditions. Verify whether a device or component reset is the best course of action before performing the following procedures.

Procedure 15-1 To reset an eNodeB



Caution — Resetting an eNodeB is service-affecting.

- 1 Perform Procedure [7-1](#) to open the ENB Equipment properties form of an eNodeB.
 - 2 Click on the Reset button. A dialog box appears.
 - 3 Enable the check box and click on the Yes button. The 5620 SAM sends the reset request to the NE.
-

Procedure 15-2 To reset an eNodeB base band card or control board card



Caution — Resetting eNodeB components is service-affecting.

- 1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment list form opens.
- 2 Choose Card→IO Card→Base Card (Physical Equipment) from the object type drop-down list.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of cards is displayed.



Note — An unfiltered search displays a list of both base band and control board cards. You can specify column filters in order to display a single card type.

- 4 Select a control board card from the list and click on the Properties button. The Card Slot - x, *card_type*, Shelf - x (Edit) form opens with the General tab displayed.
 - 5 Click on the Reset button. A dialog box appears.
 - 6 Enable the check box and click on the Yes button. The 5620 SAM sends the reset request to the NE.
 - 7 Close the Card Slot - x, *card_type*, Shelf - x (Edit) form.
-

Procedure 15-3 To reset an eNodeB RRH



Caution — Resetting eNodeB components is service-affecting.

- 1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment list form opens.
- 2 Choose Remote Radio Head (LTE) from the object type drop-down list.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of RRHs is displayed.
- 4 Select a RRH from the list and click on the Properties button. The Remote Radio Head (Edit) form opens with the General tab displayed.
- 5 Click on the Reset button. A dialog box appears.

- 6 Enable the check box and click on the Yes button. The 5620 SAM sends the reset request to the NE.
 - 7 Close the Remote Radio Head (Edit) form.
-

Procedure 15-4 To reset an eNodeB TRDU



Caution — Resetting eNodeB components is service-affecting.

- 1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
 - 2 Locate the appropriate eNodeB in the navigation tree and expand the Rack objects to display a TRDU.
 - 3 Right-click on the TRDU object and choose Properties from the contextual menu. The Transceiver Duplexer Unit (Edit) form opens with the General tab displayed.
 - 4 Click on the Reset button. A dialog box appears.
 - 5 Enable the check box and click on the Yes button. The 5620 SAM sends the reset request to the NE.
 - 6 Close the Transceiver Duplexer Unit (Edit) form.
-

Procedure 15-5 To reset an eNodeB tower mounted amplifier



Caution — Resetting eNodeB components is service-affecting.

- 1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
- 2 Locate the appropriate eNodeB in the navigation tree and expand the Rack objects to display an RFM object (either RRH or TRDU).
- 3 Right-click on the RFM and choose Properties from the contextual menu. The Remote Radio Head (Edit) or Transceiver Duplexer Unit (Edit) form opens with the General tab displayed.
- 4 Click on the Tower Mounted Amplifier tab button.
- 5 Select a tower mounted amplifier object from the list and click on the Properties button. The Tower Mounted Amplifiers (TMA) (Edit) form opens with the General tab displayed.

- 6 Click on the Reset button. A dialog box appears.
 - 7 Enable the check box and click on the Yes button. The 5620 SAM sends the reset request to the NE.
 - 8 Close the forms, as required.
-

Procedure 15-6 To reset an eNodeB remote electrical tilt



Caution — Resetting eNodeB components is service-affecting.

- 1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
 - 2 Locate the appropriate eNodeB in the navigation tree and expand the Rack objects to display an RFM object (either RRH or TRDU).
 - 3 Right-click on the RFM and choose Properties from the contextual menu. The Remote Radio Head (Edit) or Transceiver Duplexer Unit (Edit) form opens with the General tab displayed.
 - 4 Click on the Remote Electrical Tilt tab button.
 - 5 Select a remote electrical tilt object from the list and click on the Properties button. The Remote Electrical Tilt (RET) (Edit) form opens with the General tab displayed.
 - 6 Click on the Reset button. A dialog box appears.
 - 7 Enable the check box and click on the Yes button. The 5620 SAM sends the reset request to the NE.
 - 8 Close the forms, as required.
-

15.4 Event logging

The eNodeB events log records the NE fault, event, and state change history. Alarms and events (alarms with a severity of notApplicable) are included in the events log. Logged events are maintained in the 5620 SAM database according to the active log policy for the device. The events log displays entries for the following events:

- attribute value changes
- communications alarms
- environmental alarms
- equipment alarms
- device resets
- integrity violations
- miscellaneous events
- relationship changes
- state changes
- object creation events
- object deletion events
- operational violations
- physical violations
- processing error alarms
- quality of service alarms
- security service violations
- time domain violations
- unknown events

See Procedures [15-7](#) and [15-8](#) for more information about viewing the events log and configuring the active log policy. See the *5620 SAM Alarm Reference* for more information about eNodeB alarms and events.

Event logging procedures

Perform the following procedures to troubleshoot using the events log.

Procedure 15-7 To view the events log for an eNodeB

- 1 Perform Procedure [7-1](#) to open the ENB Equipment properties form of an eNodeB.
- 2 Click on the Events Log tab button.
- 3 Configure the filter criteria, if required, and click on the Search button. A list of logged events is displayed.

Procedure 15-8 To configure the event log policy for an eNodeB

- 1 Perform Procedure [7-1](#) to open the ENB Equipment properties form of an eNodeB.
- 2 Click on the Events Log tab button.
- 3 Click on the Log Policy button. The Statistics Policy - lte.Events Log form opens.
- 4 Configure the following parameters:
 - Retention Time (hours)
 - Administrative State
- 5 Click on the OK button. A confirmation form opens.

- 6 Click on the Yes button to confirm the changes.
 - 7 Close the ENB Equipment form.
-

Procedure 15-9 To purge the statistics records

Perform this procedure to purge the events log of a set of events according to an advanced filter. See the *5620 SAM User Guide* for more information about performing advanced searches and creating advanced filters.

- 1 Perform Procedure 7-1 to open the ENB Equipment properties form of an eNodeB.
 - 2 Click on the Events Log tab button.
 - 3 Click on the Log Policy button.
 - 4 Click on the More Actions button and choose Purge Statistics Records. The Statistics Policy - Lte.Events Log Filter form opens.
 - 5 Perform one of the following:
 - a Define filter criteria to specify the event type or types that will be purged. Go to step 6.
 - b Load an existing filter:
 - i Click on the Saved Filters button. The Saved Filters form opens.
 - ii Choose a filter from the list and click on the Load button. The Saved Filters form closes and the filter criteria is displayed in the Statistics Policy - Lte.Events Log Filter form. Go to step 6.
 - 6 Click on the OK button. A confirmation form opens.
 - 7 Click on the Yes button to confirm the delete action and purge the statistics record in accordance to the defined filter criteria.
 - 8 Close the Statistics Policy - Lte.Events Log form.
 - 9 Close the ENB Equipment form.
-

15.5 Device configuration and database troubleshooting

The 5620 SAM tracks eNodeB configuration change events by monitoring an incremental change counter on the NE. The 5620 SAM interprets eNodeB configuration and database errors by comparing the counter value on the device against the value in the 5620 SAM database. The 5620 SAM can set an eNodeB into the following three error states based on change counter values:

- configuration misalignment
- database fallback
- database corruption



Note — The Resync button in the device Properties form and the Discovery Manager form is dimmed when an eNodeB is in one of the three error states listed above. You must resolve the error state by performing one of the procedures in this section before you can resynchronize an eNodeB using the standard 5620 SAM resynchronization function.

Configuration misalignment

Configuration alignment errors occur when a program that is external to the 5620 SAM modifies an eNodeB parameter. An externally initiated device modification causes the value of the change counter to become greater than the value in the 5620 SAM database. The 5620 SAM raises a major configuration misalignment alarm and prevents any further configuration attempts on the faulted device until the alarm condition is resolved by an operator.

Perform one of the following actions to resolve a node configuration misalignment alarm:

- Reconfigure the device by performing Procedure [15-10](#). This action replaces the current eNodeB database configuration with the device configuration in the 5620 SAM database.
- Perform a full resynchronization by performing Procedure [15-11](#). This action replaces the device configuration in the 5620 SAM database with the current configuration in the eNodeB database.

Database fallback

The eNodeB can revert its current database configuration to a previous configuration in the event of a database error or other fault. Device fallback causes the value of the change counter to become lower than the value in the 5620 SAM database. The 5620 SAM raises a major database fallback alarm and prevents any further configuration attempts on the faulted device until the alarm condition is resolved by an operator.

Perform one of the following actions to resolve a node database fallback alarm:

- Reconfigure the device by performing Procedure 15-10. This action replaces the current eNodeB database configuration with the device configuration in the 5620 SAM database.
- Perform a full resynchronization by performing Procedure 15-11. This action replaces the device configuration in the 5620 SAM database with the current configuration in the eNodeB database.

Database corruption

The eNodeB MIM can experience unexpected errors and become corrupted. When an eNodeB resets and cannot recover the NetConf objects of the device database, the change counter on the device has a value of zero and the 5620 SAM raises a critical database corruption alarm. You can issue a reconfigure command using the 5620 SAM to replace the corrupted MIM with a previously synchronized configuration that exists in the 5620 SAM database.

Perform Procedure 15-10 to reconfigure the ENBEquipment base configuration of an eNodeB.

Configuration and database troubleshooting procedures

Perform the following procedures to troubleshoot eNodeB database errors.

Procedure 15-10 To reconfigure an eNodeB database configuration

Perform this procedure to replace the eNodeB MIM with the most recently synchronized version existing in the 5620 SAM database.



Caution 1 — Reconfiguring the eNodeB database configuration replaces the entire eNodeB NetConf MIM, regardless of the existing configuration on the device.

Caution 2 — Performing this procedure may cause a device reset, which is service-affecting.

- 1 Perform one of the following:
 - a Open the Network Element form of the faulted device using the navigation tree.
 - i Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.
 - ii Right-click on an eNodeB and choose Properties from the contextual menu. The Network Element form opens with the General tab displayed. Go to step 2.
 - b Open the Network Element form of the faulted device using the Alarm window.
 - i Locate the appropriate equipment alarm in the alarm window.
 - ii Right-click on the alarm and choose Show Affected Object from the contextual menu. The Network Element form opens with the General tab displayed. Go to step 2.
 - 2 Click on the More Actions button and choose Reconfigure NE. A warning form opens.
 - 3 Select the check box to indicate that you acknowledge the implications of the action and click on the Yes button.
 - 4 Wait for the reconfigure action to complete. This may take several minutes.
 - 5 Verify that the affecting alarm is cleared and that the eNodeB returns to a managed state.
-

Procedure 15-11 To resynchronize an eNodeB database configuration

Perform this procedure to resynchronize the current eNodeB MIM database configuration with the 5620 SAM and accept the device configuration.



Caution — Performing this procedure will replace the device configuration in the 5620 SAM database with the configuration that exists on the device. Verify that the device is functioning properly before performing this procedure.

- 1 Perform one of the following:
 - a Open the Network Element form of the faulted device using the navigation tree.
 - i Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.
 - ii Right-click on an eNodeB and choose Properties from the contextual menu. The Network Element form opens with the General tab displayed. Go to step 2.
 - b Open the Network Element form of the faulted device using the Alarm window.
 - i Locate the appropriate equipment alarm in the alarm window.
 - ii Right-click on the alarm and choose Show Affected Object from the contextual menu. The Network Element form opens with the General tab displayed. Go to step 2.
 - 2 Click on the More Actions button and choose Full Resync. A warning form opens.
 - 3 Select the check box to indicate that you acknowledge the implications of the action and click on the Yes button.
 - 4 Wait for the resynchronization to complete. This may take several minutes.
 - 5 Verify that the affecting alarm is cleared and that the eNodeB returns to a managed state.
-

15.6 Call trace

The 5620 SAM supports call trace on eNodeBs. Call trace is a function that collects call-level data on an interface. This data can be transferred to an external system for processing and analysis, and the resulting information can help a network operator do things such as the following:

- identify performance issues that may affect end-user QoS or SLAs
- troubleshoot device malfunctions

- monitor resource usage for capacity management
- validate end-to-end network transmission



Note – Call trace requires the following 5620 SAM modules:

- 5620 SAM-A
- 5620 SAM-E
- 5620 SAM-P

The 5620 SAM supports the following call trace session types:

- cell-based—a trace that the 5620 SAM initiates at operator request or as a scheduled task
- event-based—a trace that begins when a specified threshold value is reached
- signaling-based—a trace that the 9471 MME initiates
- debug—a troubleshooting trace performed by Alcatel-Lucent technical support



Note 1 – An eNodeB rejects a signaling-based call trace activation request if another type of call trace session is active.

Note 2 – An eNodeB deactivates a signaling-based call trace session if it receives a request to activate another type of call trace session.

Note 3 – You cannot manually activate an event-based session.

The 5620 SAM requires at least one pair of dedicated auxiliary servers to collect and store call trace data. The auxiliary servers are specified during a 5620 SAM main server installation or upgrade. You can use a 5620 SAM client to statically assign an eNodeB to an auxiliary server pair for call trace operations; otherwise, the 5620 SAM makes the assignment automatically when it tries to initiate a call trace session.

An auxiliary server stores call trace data files for a time specified in the general call trace configuration. However, the 5620 SAM monitors the call trace disk usage; it raises an alarm when the disk usage reaches 80%, and automatically removes the oldest call trace files when the usage reaches 95%.

You can configure and manage general call trace functions using a 5620 SAM GUI or OSS client. The Manage Call Trace Sessions GUI form allows you to do the following:

- Create, modify, and delete sessions.
- Activate or deactivate sessions.
- List and view the active sessions.
- Create call trace scheduled tasks.
- Specify the storage criteria for the collected data.

You can use the Subscriber and Equipment Traces object in the components tree of an eNodeB NE Instance properties form to configure and manage call trace functions for a specific eNodeB.

You can associate eNodeBs with call trace auxiliary-server pairs from the 5620 SAM System Information form.

Call trace scheduled tasks

You can schedule call trace session execution by creating a call trace scheduled task. A call trace scheduled task associates an existing call trace session with two 5620 SAM schedules: one that specifies when the session starts, and one that specifies when the session stops.

The following restrictions apply to a call trace session that is associated with a scheduled task:

- You cannot manually activate or deactivate the session when the task is running.
- If the session is already running at the scheduled start time, the 5620 SAM cannot execute the task, and raises an alarm against the session.
- The task deactivates the session at the scheduled stop time only if the task initiates the session.

See Scheduling chapter of the *5620 SAM User Guide* for information about 5620 SAM schedules and scheduled tasks.

Alarms

The 5620 SAM raises an alarm when it detects a call trace condition such as the following:

- excessive auxiliary-server disk-space consumption
- session or scheduled task deployment failure
- session or scheduled task execution failure
- session interruption
- invalid session or auxiliary-server configuration
- data collection, storage, or synchronization failure

Statistics

The 5620 SAM logs call trace collection performance statistics such as the following:

- packets processed
- malformed packets
- dropped packets
- files created
- files closed
- files deleted after retention time elapses

Security

Call trace involves sensitive data. Access to the associated GUI forms and to the actions that you can perform are controlled using 5620 SAM scope of command permissions.

Call trace session and scheduled task actions, for example, creation, activation, deactivation, and deletion, are recorded in the 5620 SAM User Request Log. Access to the User Request Log entries associated with call trace functions are also controlled using 5620 SAM scope of command permissions.

The `lte.SubscAndEquipmentTraces` permission controls access to call trace sessions and scheduled tasks. Table 15-1 lists the `lte.SubscAndEquipmentTraces` access types that are required for call trace actions.

Table 15-1 Call trace actions and `lte.SubscAndEquipmentTraces` access

Action	Access required
Create call trace sessions and scheduled tasks	Create
Activate call trace sessions and scheduled tasks Deactivate call trace sessions and scheduled tasks	Update/Execute
Delete call trace sessions and scheduled tasks	Delete

Data collection and storage

During a call trace session, an eNodeB sends messages in UPOS format over UDP to the Preferred auxiliary server, which converts the message content to 3GPP XML format and adds it to a call trace file. After a specified rollover time, or when the session ends, the auxiliary server compresses the file using gzip and saves it on the local file system. The Preferred auxiliary server synchronizes the call trace data files with the Reserved auxiliary server.



Note — The call trace storage directories that you configure on the Preferred and Reserved auxiliary servers in a pair must match, or data synchronization between the servers fails.

The call trace data files are stored in the following directory on an auxiliary server:

base_directory/A_sender/trace_reference

where

base_directory is the call trace receiving directory specified during 5620 SAM auxiliary-server installation or upgrade, typically `/opt/5620sam/calltrace`

sender is the eNodeB identifier

trace_reference is the UPOS trace reference

A call trace file name has the following format:

`YYYYMMDD.HHMMoffseteNodeB.sender.reference.session.gz`

where

YYYYMMDD is the collection date of the first record in the file

HHMM is the collection time of the first record in the file

offset is the offset from UTC in the format *signHHMM* for example, +0300

sender is the unique UPOS name of the eNodeB

reference is the UPOS trace reference, a hexadecimal value in which the high-order three bytes are the MCC and MNC, and the low-order three bytes are the trace ID

session is the UPOS trace recording session reference value, in decimal



Note — The name of a call trace file is prepended with TMP_ when the file is in use for data collection. You cannot open or process a call trace file that is in use for data collection.

Call trace management procedures

The following procedures describe how to configure global 5620 SAM and local eNodeB call trace functions. See the *5620 SAM LTE Parameter Reference* for more information about the parameters in the following procedures.

Procedure 15-12 To configure global 5620 SAM call trace operation

Perform this procedure to configure the 5620 SAM call trace operational parameters.

- 1 Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions form opens with the General tab displayed.
 - 2 Configure the parameters:
 - Call Trace UDP Port
 - File Retention Time (hrs)
 - File Rollover Time (min)
 - Disk Usage Alarm Threshold
 - Disk Usage Alarm Severity
 - 3 Click on the OK button. A dialog box appears.
 - 4 Click on the Yes button. The Manage Call Trace Sessions form closes.
-

Procedure 15-13 To configure local eNodeB call trace operation

Perform this procedure to configure the call trace operational parameters on an eNodeB.

- 1 Choose Manage→Mobile Access→eNodeB Logical Objects from the 5620 SAM main menu. The Manage eNodeB Logical Objects form opens with the General tab displayed.
- 2 Choose eNodeB NE Instance (LTE) from the Select Object Type drop-down list and click on the Search button. A list of eNodeB NE instances is displayed.

- 3 Select an eNodeB NE instance in the list and click on the Properties button. The eNodeB NE Instance (Edit) form opens with the General tab displayed.
- 4 Click on the Components tab button.
- 5 Navigate to a Subscriber and Equipment Traces object. The path is eNodeB NE Instance→Subscriber and Equipment Traces→Subscriber and Equipment Traces ID *n*.
- 6 Right-click on the Subscriber and Equipment Traces ID *n* object and choose Properties from the contextual menu. The Subsc and Equipment Traces (Edit) form opens with the General tab displayed.
- 7 Configure the parameters:



Note — The isPCMDEnabled parameter consumes a RAN license token from the LTEisPCMDEnabled feature entitlement when the parameter is enabled. See Chapter 9 for more information about RAN licensing.

- isPCMDEnabled
 - isSignBasedCTEnabled
- 8 Click on the OK button. The Subsc and Equipment Traces (Edit) form closes.
 - 9 Click on the Yes button. The Manage Call Trace Sessions form closes.

Procedure 15-14 To create a call trace session using the global call trace management form

Perform this procedure to create a call trace session for manual or scheduled activation using the Manage Call Trace Sessions form.

- 1 Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions form opens with the General tab displayed.
- 2 Click on the Call Trace Sessions tab button.
- 3 Click on the Create button. The Call Trace Session (Create) form opens with the General tab displayed.
- 4 Enter a description for the call trace session in the Description field, if required.
- 5 Click on the Select button to choose an eNodeB instance for the call trace session. The Select eNodeB Instance form opens.
- 6 Select an eNodeB instance in the list and click on the OK button. The Select eNodeB Instance form closes, and the eNodeB instance is displayed on the Call Trace Session (Create) form.

- 7 Configure the parameters:
 - Auto-Assign ID
 - traceId
 - callTraceSessionName
 - isRRCTraced
 - isS1MMETraced
 - isX2Traced
 - trafficThreshold (%)
 - rrcReestablishmentThreshold
 - iratHThreshold
 - 8 Click on the List of Traced Cells tab button.
 - 9 Click on the Add button. The Select Cells for Call Trace Session form opens with a list of available cells.
 - 10 Select one or more cells in the list and click on the OK button. The Select Cells for Call Trace Session form closes, and the cells are listed on the Call Trace Session (Create) form.
 - 11 Click on the OK button. A dialog box appears.
 - 12 Click on the Yes button. The Call Trace Session (Create) form closes.
 - 13 Close the Manage Call Trace Sessions form.
-

Procedure 15-15 To create a call trace session using an eNodeB instance properties form

Perform this procedure to create a call trace session for manual or scheduled activation using an eNodeB instance properties form.

- 1 Choose Manage→Mobile Access→eNodeB Logical Objects from the 5620 SAM main menu. The Manage eNodeB Logical Objects form opens with the General tab displayed.
- 2 Choose eNodeB NE Instance (LTE) from the Select Object Type drop-down list and click on the Search button. A list of eNodeB NE instances is displayed.
- 3 Select an eNodeB NE instance in the list and click on the Properties button. The eNodeB NE Instance (Edit) form opens with the General tab displayed.
- 4 Click on the Components tab button.
- 5 Navigate to a call trace object. The path is eNodeB NE Instance→Subscriber and Equipment Traces→Subscriber and Equipment Traces ID *n*→Ctg.
- 6 Right-click on the Ctg object and choose Create Call Trace Session from the contextual menu. The Call Trace Session (Create) form opens with the General tab displayed.

- 7 Configure the parameters:
 - Auto-Assign ID
 - traceId
 - callTraceSessionName
 - isRRCTraced
 - isS1MMETraced
 - isX2Traced
 - trafficThreshold (%)
 - rrcReestablishmentThreshold
 - iratHOTThreshold
 - 8 Click on the List of Traced Cells tab button.
 - 9 Click on the Add button. The Select Cells for Call Trace Session form opens with a list of available cells.
 - 10 Select one or more cells in the list and click on the OK button. The Select Cells for Call Trace Session form closes, and the cells are listed on the Call Trace Session (Create) form.
 - 11 Click on the OK button. A dialog box appears.
 - 12 Click on the Yes button. The Call Trace Session (Create) form closes, and a new CTg ID: *n* object is displayed in the eNodeB instance components tree.
 - 13 Click on the OK button. A dialog box appears.
 - 14 Click on the Yes button. The eNodeB NE Instance (Edit) form closes.
 - 15 Close the Manage eNodeB Logical Objects form.
-

Procedure 15-16 To activate a call trace session

Perform this procedure to manually activate an existing call trace session.



Note — You cannot activate a call trace session when the session is currently running as part of a scheduled task.

- 1 Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions form opens with the General tab displayed.
- 2 Click on the Call Trace Sessions tab button. The tab lists the available call trace sessions.

- 3 Select a call trace session in the list and click on the Activate button. The call trace session is activated.
 - 4 Close the Manage Call Trace Sessions form.
-

Procedure 15-17 To deactivate a call trace session

Perform this procedure to manually deactivate an active call trace session.



Note — You cannot deactivate a call trace session when the session is currently running as part of a scheduled task.

- 1 Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions form opens with the General tab displayed.
 - 2 Click on the Call Trace Sessions tab button. The tab lists the available call trace sessions.
 - 3 Select a call trace session in the list and click on the Deactivate button. The call trace session is deactivated.
 - 4 Close the Manage Call Trace Sessions form.
-

Procedure 15-18 To delete a call trace session

Perform this procedure to delete a call trace session from the 5620 SAM.

- 1 Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions form opens with the General tab displayed.
 - 2 If the call trace session is associated with a scheduled task, you must delete the scheduled task before you can delete the call trace session. Perform the following steps.
 - i Click on the Scheduled Call Trace Sessions tab button.
 - ii Select the scheduled task associated with the call trace session.
 - iii If the scheduled task is running, click on the Task Action button and choose Stop. The scheduled task execution stops.
 - iv Click on the Task Action button and choose Shut Down. The Delete button is enabled.
 - v Click on the Delete button. A dialog box appears.
 - vi Click on the Yes button. The 5620 SAM deletes the scheduled task.
 - 3 Click on the Call Trace Sessions tab button.
-

- 4 Select the call trace session in the list.
 - 5 If the call trace session is running, click on the Deactivate button. The call trace session is deactivated.
 - 6 Click on the Properties button. The Call Trace Session (Edit) form opens.
 - 7 Set the Administrative State parameter to Disabled.
 - 8 Click on the OK button. The Call Trace Session (Edit) form closes.
 - 9 Click on the Delete button. A dialog box appears.
 - 10 Click on the Yes button. The 5620 SAM deletes the call trace session.
 - 11 Select a call trace session in the list and click on the Delete button. The call trace session is deleted.
 - 12 Close the Manage Call Trace Sessions form.
-

Procedure 15-19 To create a call trace scheduled task

Perform this procedure to enable the execution of a call trace session according to a schedule.

- 1 Create the following 5620 SAM schedules:
 - a start schedule that defines when the call trace is to be activated
 - a stop schedule that defines when the call trace is to be deactivated

See Scheduling chapter of the *5620 SAM User Guide* for information about creating schedules.
- 2 Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions form opens with the General tab displayed.
- 3 Click on the Scheduled Call Trace Sessions tab button.
- 4 Click on the Create button. The Call Trace Scheduled Task form opens with the General tab displayed.
- 5 Configure the parameters:
 - Scheduled Task Name
 - Scheduled Task Description
 - Administrative State

- 6 Perform the following steps to choose a start schedule.
 - i Click on the Select button in the Start Schedule panel. The Select Start Schedule - Call Trace Scheduled Task form opens.
 - ii Select a schedule in the list and click on the OK button. the Select Start Schedule - Call Trace Scheduled Task form closes, and the schedule identifiers are displayed on the Call Trace Scheduled Task form.
 - 7 Perform the following steps to choose a stop schedule.
 - i Click on the Select button in the Stop Schedule panel. The Select Stop Schedule - Call Trace Scheduled Task form opens.
 - ii Select a schedule in the list and click on the OK button. the Select Stop Schedule - Call Trace Scheduled Task form closes, and the schedule identifiers are displayed on the Call Trace Scheduled Task form.
 - 8 Click on the Call Trace Sessions tab button.
 - 9 Click on the Add button. The Select Call Trace Sessions for Call Trace Scheduled Task form opens with a list of available call trace sessions listed.
 - 10 Select a call trace session and click on the OK button. The Select Call Trace Sessions for Call Trace Scheduled Task form closes, and the call trace session is listed on the Call Trace Scheduled Task form.
 - 11 Click on the OK button. A dialog box appears.
 - 12 Click on the Yes button. The Call Trace Scheduled Task (Create) form closes, and the call trace scheduled task is listed on the Manage Call Trace Sessions form.
 - 13 Close the Manage Call Trace Sessions form.
-

Procedure 15-20 To control call trace scheduled task execution

Perform this procedure to start, stop, enable, or disable a call trace scheduled task.

- 1 Choose Manage→Mobile Access→Call Trace Sessions from the 5620 SAM main menu. The Manage Call Trace Sessions form opens with the General tab displayed.
- 2 Click on the Scheduled Call Trace Sessions tab button.
- 3 Select a scheduled task in the list.
- 4 Click on the Task Action button and perform one of the following using a contextual menu option.
 - a To immediately execute the scheduled task, choose Start Session.
 - b To immediately stop scheduled task execution, choose Stop.

- c To administratively enable the scheduled task, choose Turn Up.
 - d To administratively disable the scheduled task, choose Shut Down.
- 5 Close the Manage Call Trace Sessions form.

Procedure 15-21 To manage the assignment of eNodeBs to call trace auxiliary-server pairs

Perform this procedure to specify which eNodeBs are assigned to which call trace auxiliary-server pairs.

- 1 Choose Administration->System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.
- 2 Click on the Auxiliary Service Server Pair Group tab button.
- 3 Select an auxiliary-server pair group in the list and click on the Properties button. The Auxiliary Service Server Pair Group form opens with the General tab displayed.
- 4 Click on the Auxiliary Server Pair tab button.
- 5 Select an auxiliary-server pair in the list and click on the Properties button. The Auxiliary Server Pair form opens with the General tab displayed.
- 6 Click on the Assigned Objects tab button. The Assigned Objects tab lists the eNodeBs that are assigned to the auxiliary-server pair.
- 7 To assign an eNodeB to the auxiliary-server pair, perform the following steps.
 - i Click on the Add button. The Select Network Elements form opens.
 - ii Select an eNodeB in the list and click on the OK button. The Select Network Elements form closes, and the eNodeB is listed on the Auxiliary Server Pair form.
- 8 To remove an assigned eNodeB from the auxiliary-server pair, click on the Delete button. The eNodeB is removed from the list.
- 9 Click on the OK button. The Auxiliary Server Pair form closes.
- 10 Click on the OK button. A dialog box appears.
- 11 Click on the Yes button. The Auxiliary Server Pair form closes.
- 12 Close the System Information form.

After you assign an eNodeB to a different auxiliary-server pair, the 5620 SAM updates the auxiliary-server IP address on the Subsc And Equipment Traces form of the eNodeB.

After you remove an assigned eNodeB from an auxiliary-server pair, the 5620 SAM replaces the auxiliary-server IP address on the Subsc And Equipment Traces form of the eNodeB with a series of zeroes.

- 13 Close the Manage Call Trace Sessions form.
-

Appendices

A. eNodeB PM statistics counters *A-1*

B. RAN licenses *B-1*

A. *eNodeB PM statistics counters*

A.1 eNodeB PM statistics counters A-2

A.2 eNodeB interface statistics A-80

A.1 eNodeB PM statistics counters

This appendix lists in tabular form the PM statistics counters that the 5620 SAM supports for the eNodeB. The tables are organized by PM counter class and list the counters and subcounters by the standardized 3GPP name. Some counters have subcounters, which are indicated using a period and 3GPP suffix that are appended to the parent counter eNodeB 3GPP name. For example, VS.IfInLinkUtilisation.Max is a subcounter of the VS.IfInLinkUtilisation counter.

See the *Alcatel-Lucent 9412 eNodeB Counters Reference Guide 418-000-035* for descriptive information about eNodeB PM statistics counters.

Table A-1 lists each statistics class and the associated statistics-counter table.

Table A-1 Statistics classes and counter tables

Counter class name	See
Active users Stats	A-2
Additional E-RAB Setup Stats	A-3
CS Fallback Cell Change Order To GERAN	A-4
CS Fallback PS Handover To UTRAN FDD	A-5
Cell Change Order To GERAN	A-6
Cell Throughput On L1 Channels Stats	A-7
Common Mobility Management Framework Stats	A-8
Control format indicator usage	A-9
DL PRB Usage Stats	A-10
Downlink Cell PDCP SDU Volume Stats	A-11
Downlink Grants per TTI Stats	A-12
Downlink L2 Traffic and Throughput Stats	A-13
Downlink MIMO eligibility decisions Stats	A-14
Dynamic Scheduling Stats	A-15
E-RAB Abnormal Release Stats	A-16
E-RAB Modify Failure Stats	A-17
E-RAB Modify Request Stats	A-18
E-RAB Modify Success Stats	A-19
E-RAB Normal Release Stats	A-20
E-RAB Release Command E-RAB Requested To Be Released Stats	A-21
E-RAB Release Indication E-RAB Released Stats	A-22
E-RAB Release Response E-RAB Release Stats	A-23
E-RAB Setup Procedure Stats	A-24
ENB Sync And Announce Message Stats	A-25
Enhanced Non-Optimized Redirections To HRPD Via Event B2 Stats	A-26

(1 of 6)

Counter class name	See
GBR E-RAB Stats	A-27
GEthernet interface Stats	A-28
Gap-Assisted Handover Stats	A-29
HO Cell Selection Stats	A-30
HO Inter-Cell Intra-eNodeB Stats	A-31
HO Intra-Cell Stats	A-32
Incoming E-RAB Setup Stats	A-33
Incoming E-RAB To Be Setup On IRATHO Stats	A-34
Incoming HO Inter-Cell Inter-eNodeB via S1 Stats	A-35
Incoming HO Inter-Cell Inter-eNodeB via X2 Stats	A-36
Incoming HO Inter-Cell Intra-eNodeB Stats	A-37
Incoming PS Handover From UTRA Stats	A-38
Initial E-RAB Setup Stats	A-39
L1 Connection Stats	A-40
L1 Traffic and throughput MAC-BLER	A-41
Layer 0 wideband CQI reported in MIMO Stats	A-42
Layer 1 wideband CQI reported in MIMO Stats	A-43
Local UE Context Release Stats	A-44
Non-GBR E-RAB RLC Downlink Throughput Stats	A-45
Non-GBR E-RAB RLC Uplink Throughput Stats	A-46
Number Of Bearers Per Cell	A-47
Number Of Bearers Per eNodeB	A-48
OAM VLAN Stats	A-49
Outgoing HO Inter-Cell Inter-eNodeB via S1 Stats	A-50
Outgoing HO Inter-Cell Inter-eNodeB via X2 Stats	A-51
Outgoing HO Inter-Cell Intra-eNodeB Stats	A-52
Outgoing PS Handover To UTRAN FDD	A-53
Outgoing PS Handover To UTRAN FDD Failure And Abort Stats	A-54
Outgoing PS Handover To UTRAN TDD	A-55
PRBs Pool Overload Stats	A-56
PS Handover to UTRAN FDD Stats	A-57
PS Handover to UTRAN TDD Stats	A-58
Paging Attempt Stats	A-59
Power Headroom Stats	A-60
RACH	A-61
RRC Connection Release Due To MME Overload	A-62
RRC Connection Setup Stats	A-63

(2 of 6)

Counter class name	See
RRC Connection Stats	A-64
RRC Reestablishment Setup Stats	A-65
Radio Link Stats	A-66
Redirection To HRPD Stats	A-67
Redirection To Inter-Frequency Intra-FDD or TDD Stats	A-68
Redirection To Inter-Frequency Same Frame Structure Stats	A-69
Redirection to GERAN Stats	A-70
Redirection to UTRAN FDD Stats	A-71
Redirection to UTRAN TDD Stats	A-72
S1 Error Indication By MME Stats	A-73
S1 Error Indication By eNodeB Stats	A-74
S1 SCTP Traffic Stats	A-75
S1 Setup Stats	A-76
SCTP Association Stats	A-77
Throughput On S1 interfaces Stats	A-78
Throughput On X2 interfaces Stats	A-79
Traffic On S1 interfaces Stats	A-80
Traffic On X2 interfaces Stats	A-81
Transport Block Stats	A-82
UE Context Modification Stats	A-83
UE Context Release Command Stats	A-84
UE Context Release Request Stats	A-85
UE Context Setup Stats	A-86
UE scheduled per TTI Stats	A-87
UL PRB Usage Stats	A-88
Uplink Cell PDCP SDU Volume Stats	A-89
Uplink Grants per TTI Stats	A-90
Uplink L2 Traffic and Throughput Stats	A-91
Uplink Noise For PRB1	A-92
Uplink Noise For PRB10	A-93
Uplink Noise For PRB100	A-94
Uplink Noise For PRB11	A-95
Uplink Noise For PRB12	A-96
Uplink Noise For PRB13	A-97
Uplink Noise For PRB14	A-98
Uplink Noise For PRB15	A-99
Uplink Noise For PRB16	A-100

(3 of 6)

Counter class name	See
Uplink Noise For PRB17	A-101
Uplink Noise For PRB18	A-102
Uplink Noise For PRB19	A-103
Uplink Noise For PRB2	A-104
Uplink Noise For PRB20	A-105
Uplink Noise For PRB21	A-106
Uplink Noise For PRB22	A-107
Uplink Noise For PRB23	A-108
Uplink Noise For PRB24	A-109
Uplink Noise For PRB25	A-110
Uplink Noise For PRB26	A-111
Uplink Noise For PRB27	A-112
Uplink Noise For PRB28	A-113
Uplink Noise For PRB29	A-114
Uplink Noise For PRB3	A-115
Uplink Noise For PRB30	A-116
Uplink Noise For PRB31	A-117
Uplink Noise For PRB32	A-118
Uplink Noise For PRB33	A-119
Uplink Noise For PRB34	A-120
Uplink Noise For PRB35	A-121
Uplink Noise For PRB36	A-122
Uplink Noise For PRB37	A-123
Uplink Noise For PRB38	A-124
Uplink Noise For PRB39	A-125
Uplink Noise For PRB4	A-126
Uplink Noise For PRB40	A-127
Uplink Noise For PRB41	A-128
Uplink Noise For PRB42	A-129
Uplink Noise For PRB43	A-130
Uplink Noise For PRB44	A-131
Uplink Noise For PRB45	A-132
Uplink Noise For PRB46	A-133
Uplink Noise For PRB47	A-134
Uplink Noise For PRB48	A-135
Uplink Noise For PRB49	A-136
Uplink Noise For PRB5	A-137

(4 of 6)

Counter class name	See
Uplink Noise For PRB50	A-138
Uplink Noise For PRB51	A-139
Uplink Noise For PRB52	A-140
Uplink Noise For PRB53	A-141
Uplink Noise For PRB54	A-142
Uplink Noise For PRB55	A-143
Uplink Noise For PRB56	A-144
Uplink Noise For PRB57	A-145
Uplink Noise For PRB58	A-146
Uplink Noise For PRB59	A-147
Uplink Noise For PRB6	A-148
Uplink Noise For PRB60	A-149
Uplink Noise For PRB61	A-150
Uplink Noise For PRB62	A-151
Uplink Noise For PRB63	A-152
Uplink Noise For PRB64	A-153
Uplink Noise For PRB65	A-154
Uplink Noise For PRB66	A-155
Uplink Noise For PRB67	A-156
Uplink Noise For PRB68	A-157
Uplink Noise For PRB69	A-158
Uplink Noise For PRB7	A-159
Uplink Noise For PRB70	A-160
Uplink Noise For PRB71	A-161
Uplink Noise For PRB72	A-162
Uplink Noise For PRB73	A-163
Uplink Noise For PRB74	A-164
Uplink Noise For PRB75	A-165
Uplink Noise For PRB76	A-166
Uplink Noise For PRB77	A-167
Uplink Noise For PRB78	A-168
Uplink Noise For PRB79	A-169
Uplink Noise For PRB8	A-170
Uplink Noise For PRB80	A-171
Uplink Noise For PRB81	A-172
Uplink Noise For PRB82	A-173
Uplink Noise For PRB83	A-174

(5 of 6)

Counter class name	See
Uplink Noise For PRB84	A-175
Uplink Noise For PRB85	A-176
Uplink Noise For PRB86	A-177
Uplink Noise For PRB87	A-178
Uplink Noise For PRB88	A-179
Uplink Noise For PRB89	A-180
Uplink Noise For PRB9	A-181
Uplink Noise For PRB90	A-182
Uplink Noise For PRB91	A-183
Uplink Noise For PRB92	A-184
Uplink Noise For PRB93	A-185
Uplink Noise For PRB94	A-186
Uplink Noise For PRB95	A-187
Uplink Noise For PRB96	A-188
Uplink Noise For PRB97	A-189
Uplink Noise For PRB98	A-190
Uplink Noise For PRB99	A-191
Uplink Paired Grants per TTI Stats	A-192
VoIP downlink FER Stats	A-193
Wideband CQI Reported in Tx Diversity Stats	A-194
X2 SCTP Traffic Stats	A-195

(6 of 6)

Table A-2 Active users Stats

PM counter 3GPP name
VS.NbActiveUEInULPerQCI.VoIP
VS.NbActiveUEInULPerQCI.GBR
VS.NbActiveUEInULPerQCI.NonGBR
VS.NbActiveUEInULPerQCI
VS.NbActiveUEInDLPerQCI.VoIP
VS.NbActiveUEInDLPerQCI.GBR
VS.NbActiveUEInDLPerQCI.NonGBR
VS.NbActiveUEInDLPerQCI
Monitored class: lte.Cell

Table A-3 Additional E-RAB Setup Stats

PM counter 3GPP name
VS.AdditionalERABSetupRequest.QCI1
VS.AdditionalERABSetupRequest.QCI2
VS.AdditionalERABSetupRequest.QCI3
VS.AdditionalERABSetupRequest.QCI4
VS.AdditionalERABSetupRequest.QCI5
VS.AdditionalERABSetupRequest.QCI6
VS.AdditionalERABSetupRequest.QCI7
VS.AdditionalERABSetupRequest.QCI8
VS.AdditionalERABSetupRequest.QCI9
VS.AdditionalERABSetupRequest.CustomerQCIs
VS.AdditionalERABSetupSuccess.QCI1
VS.AdditionalERABSetupSuccess.QCI2
VS.AdditionalERABSetupSuccess.QCI3
VS.AdditionalERABSetupSuccess.QCI4
VS.AdditionalERABSetupSuccess.QCI5
VS.AdditionalERABSetupSuccess.QCI6
VS.AdditionalERABSetupSuccess.QCI7
VS.AdditionalERABSetupSuccess.QCI8
VS.AdditionalERABSetupSuccess.QCI9
VS.AdditionalERABSetupSuccess.CustomerQCIs
Monitored class: lte.Cell

Table A-4 CS Fallback Cell Change Order To GERAN

PM counter 3GPP name
VS.CsFallbackCCOToGeranAttempt.WithNACC
VS.CsFallbackCCOToGeranAttempt.WithoutNACC
VS.CsFallbackCCOToGeranAttempt
VS.CsFallbackCCOToGeranSuccess.WithNACC
VS.CsFallbackCCOToGeranSuccess.WithoutNACC
VS.CsFallbackCCOToGeranSuccess
VS.CsFallbackCCOToGeranFailureSum.WithNACC
VS.CsFallbackCCOToGeranFailureSum.WithoutNACC
VS.CsFallbackCCOToGeranFailureSum
Monitored class: lte.Cell

Table A-5 CS Fallback PS Handover To UTRAN FDD

PM counter 3GPP name
VS.OutgoingCsFallbackPSHOTOtraFddAttempt
VS.OutgoingCsFallbackPSHOTOtraFddSuccess
VS.OutgoingCsFallbackPSHOTOtraFddFailureSum
VS.OutgoingCsFallbackPSHOTOtraFddAbortSum
Monitored class: lte.Cell

Table A-6 Cell Change Order To GERAN

PM counter 3GPP name
VS.CCOToGeranAttempt.EventB2AndThreshold1RSRPThreshold2GERANWithNACC
VS.CCOToGeranAttempt.EventB2AndThreshold1RSRQThreshold2GERANWithNACC
VS.CCOToGeranAttempt.EventB2AndThreshold1RSRPThreshold2GERANWithoutNACC
VS.CCOToGeranAttempt.EventB2AndThreshold1RSRQThreshold2GERANWithoutNACC
VS.CCOToGeranAttempt
VS.CCOToGeranSuccess.EventB2AndThreshold1RSRPThreshold2GERANWithNACC
VS.CCOToGeranSuccess.EventB2AndThreshold1RSRQThreshold2GERANWithNACC
VS.CCOToGeranSuccess.EventB2AndThreshold1RSRPThreshold2GERANWithoutNACC
VS.CCOToGeranSuccess.EventB2AndThreshold1RSRQThreshold2GERANWithoutNACC
VS.CCOToGeranSuccess
VS.CCOToGeranFailureSum.withNACC
VS.CCOToGeranFailureSum.withoutNACC
VS.CCOToGeranFailureSum
VS.CCOToGeranFailure.RRCCConnectionReestablishmentInCCOwithNACC
VS.CCOToGeranFailure.RRCCConnectionReestablishmentInCCOwithoutNACC
VS.CCOToGeranFailure
Monitored class: lte.Cell

Table A-7 Cell Throughput On L1 Channels Stats

PM counter 3GPP name
VS.CellDLL1Throughput.LeRange1
VS.CellDLL1Throughput.GTRange1LeRange2
VS.CellDLL1Throughput.GTRange2LeRange3
VS.CellDLL1Throughput.GTRange3LeRange4

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.CellDLL1Throughput.GTRange4
VS.CellULL1Throughput.LeRange1
VS.CellULL1Throughput.GTRange1LeRange2
VS.CellULL1Throughput.GTRange2LeRange3
VS.CellULL1Throughput.GTRange3LeRange4
VS.CellULL1Throughput.GTRange4
Monitored class: lte.Cell

(2 of 2)

Table A-8 Common Mobility Management Framework Stats

PM counter 3GPP name
VS.EvolvedMultiCarrierTrafficAllocationTrigger.EventA2CAForGoodToAlarmTransitionForRadioCoverage
VS.EvolvedMultiCarrierTrafficAllocationTrigger
Monitored class: lte.Cell

Table A-9 Control format indicator usage

PM counter 3GPP name
VS.CFIUsage.CFI1
VS.CFIUsage.CFI2
VS.CFIUsage.CFI3
VS.CFIUsage
Monitored class: lte.Cell

Table A-10 DL PRB Usage Stats

PM counter 3GPP name
VS.DLTotalPRBUsage
VS.DLPRBUsagePerTrafficClass.VoIP
VS.DLPRBUsagePerTrafficClass.GBR
VS.DLPRBUsagePerTrafficClass.NonGBR
VS.DLPRBUsagePerTrafficClass
Monitored class: lte.Cell

Table A-11 Downlink Cell PDCP SDU Volume Stats

PM counter 3GPP name
VS.DRBPdcpSduKbytesDL.VoIP
VS.DRBPdcpSduKbytesDL.OtherGBR
VS.DRBPdcpSduKbytesDL.NonGBR
VS.DRBPdcpSduKbytesDL
VS.DRBPdcpSduBitRateDL
Monitored class: lte.Cell

Table A-12 Downlink Grants per TTI Stats

PM counter 3GPP name
VS.DLGrant.0Grant
VS.DLGrant.1Grant
VS.DLGrant.2Grants
VS.DLGrant.3Grants
VS.DLGrant.4Grants
VS.DLGrant.5Grants
VS.DLGrant.6orMoreGrants
Monitored class: lte.Cell

Table A-13 Downlink L2 Traffic and Throughput Stats

PM counter 3GPP name
VS.DLRlcPduKbytes.VoIP
VS.DLRlcPduKbytes.GBR
VS.DLRlcPduKbytes.NonGBR
VS.DLRlcPduSent.VoIP
VS.DLRlcPduSent.GBR
VS.DLRlcPduSent.NonGBR
VS.DLRlcPduRetransmitted.GBR
VS.DLRlcPduRetransmitted.NonGBR
Monitored class: lte.Cell

Table A-14 Downlink MIMO eligibility decisions Stats

PM counter 3GPP name
VS.DLMimoEligibilityDecision.Eligible
VS.DLMimoEligibilityDecision.NotEligible
VS.DLMimoEligibilityDecision
Monitored class: lte.Cell

Table A-15 Dynamic Scheduling Stats

PM counter 3GPP name
VS.DLDataVolumeWithDynamicSchedulingPerUserCategory.FDUsers
VS.DLDataVolumeWithDynamicSchedulingPerUserCategory.FSUsers
VS.ULDataVolumeWithDynamicSchedulingPerUserCategory.FDUsers
VS.ULDataVolumeWithDynamicSchedulingPerUserCategory.FSUsers
VS.DLPRBUsedWithDynamicSchedulingPerUserCategory.FDUsers
VS.DLPRBUsedWithDynamicSchedulingPerUserCategory.FSUsers
VS.ULPRBUsedWithDynamicSchedulingPerUserCategory.FDUsers
VS.ULPRBUsedWithDynamicSchedulingPerUserCategory.FSUsers
VS.PUCCHMessagesPerType.PcqiPmiRiConf
VS.PUCCHMessagesPerType.SRRec
VS.PUCCHMessagesPerType.SRConf
Monitored class: lte.Cell

Table A-16 E-RAB Abnormal Release Stats

PM counter 3GPP name
VS.AbnormalERABReleasePerQCI.QCI1
VS.AbnormalERABReleasePerQCI.QCI2
VS.AbnormalERABReleasePerQCI.QCI3
VS.AbnormalERABReleasePerQCI.QCI4
VS.AbnormalERABReleasePerQCI.QCI5
VS.AbnormalERABReleasePerQCI.QCI6
VS.AbnormalERABReleasePerQCI.QCI7
VS.AbnormalERABReleasePerQCI.QCI8
VS.AbnormalERABReleasePerQCI.QCI9
VS.AbnormalERABReleasePerQCI.CustomerQCIs

(1 of 2)

PM counter 3GPP name
Monitored class: lte.Cell

(2 of 2)

Table A-17 E-RAB Modify Failure Stats

PM counter 3GPP name
VS.ERABModifyFailed.OAMIntervention
VS.ERABModifyFailed.InvalidIECombination
VS.ERABModifyFailed.CACFailure
VS.ERABModifyFailed.InternalFailure
VS.ERABModifyFailed.Timeout
VS.ERABModifyFailed.RRCCConnectionReestablishment
VS.ERABModifyFailed.InteractionWithOtherProcedure
VS.ERABModifyFailed
Monitored class: lte.Cell

Table A-18 E-RAB Modify Request Stats

PM counter 3GPP name
VS.ERABModifyRequest.QCI1
VS.ERABModifyRequest.QCI2
VS.ERABModifyRequest.QCI3
VS.ERABModifyRequest.QCI4
VS.ERABModifyRequest.QCI5
VS.ERABModifyRequest.QCI6
VS.ERABModifyRequest.QCI7
VS.ERABModifyRequest.QCI8
VS.ERABModifyRequest.QCI9
VS.ERABModifyRequest.CustomerQCIs
VS.ERABModifyRequest
Monitored class: lte.Cell

Table A-19 E-RAB Modify Success Stats

PM counter 3GPP name
VS.ERABModifySuccess.QCI1

(1 of 2)

PM counter 3GPP name
VS.ERABModifySuccess.QCI2
VS.ERABModifySuccess.QCI3
VS.ERABModifySuccess.QCI4
VS.ERABModifySuccess.QCI5
VS.ERABModifySuccess.QCI6
VS.ERABModifySuccess.QCI7
VS.ERABModifySuccess.QCI8
VS.ERABModifySuccess.QCI9
VS.ERABModifySuccess.CustomerQCIs
VS.ERABModifySuccess
Monitored class: lte.Cell

(2 of 2)

Table A-20 E-RAB Normal Release Stats

PM counter 3GPP name
VS.NormalERABRelease.QCI1
VS.NormalERABRelease.QCI2
VS.NormalERABRelease.QCI3
VS.NormalERABRelease.QCI4
VS.NormalERABRelease.QCI5
VS.NormalERABRelease.QCI6
VS.NormalERABRelease.QCI7
VS.NormalERABRelease.QCI8
VS.NormalERABRelease.QCI9
VS.NormalERABRelease.CustomerQCIs
Monitored class: lte.Cell

Table A-21 E-RAB Release Command E-RAB Requested To Be Released Stats

PM counter 3GPP name
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI1
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI2
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI3
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI4
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI5

(1 of 2)

PM counter 3GPP name
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI6
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI7
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI8
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.QCI9
VS.ERABReleaseCommandERABRequestedToBeReleasedPerQCI.CustomerQCIs
VS.ERABReleaseCommandERABRequestedToBeReleasedPerCause.NormalRelease
VS.ERABReleaseCommandERABRequestedToBeReleasedPerCause.Unspecified
VS.ERABReleaseCommandERABRequestedToBeReleasedPerCause.OtherCause
Monitored class: lte.Cell

(2 of 2)

Table A-22 E-RAB Release Indication E-RAB Released Stats

PM counter 3GPP name
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI1
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI2
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI3
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI4
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI5
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI6
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI7
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI8
VS.ERABReleaseIndicationERABReleasedPerQCI.QCI9
VS.ERABReleaseIndicationERABReleasedPerQCI.CustomerQCIs
VS.ERABReleaseIndicationERABReleasedPerCause.NoRadioResourceAvailableInTargetCell
Monitored class: lte.Cell

Table A-23 E-RAB Release Response E-RAB Release Stats

PM counter 3GPP name
VS.ERABReleaseResponseERABReleaseSuccess
VS.ERABReleaseResponseERABReleaseFailure.UnknownERABId
VS.ERABReleaseResponseERABReleaseFailure.FailureInTheRadioInterfaceProcedure
VS.ERABReleaseResponseERABReleaseFailure.RadioConnectionWithUELost
VS.ERABReleaseResponseERABReleaseFailure.Unspecified
VS.ERABReleaseResponseERABReleaseFailure.X2HandoverTriggered

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.ERABReleaseResponseERABReleaseFailure.S1IntrasystemHandoverTriggered
VS.ERABReleaseResponseERABReleaseFailure.S1IntersystemHandoverTriggered
Monitored class: lte.Cell

(2 of 2)

Table A-24 E-RAB Setup Procedure Stats

PM counter 3GPP name
VS.ERABSetupFailed.CACFailure
VS.ERABSetupFailed.InternalFailure
VS.ERABSetupFailed.RRCCConnectionReestablishment
VS.ERABSetupFailed.Timeout
VS.ERABSetupFailed.ERABContextAllocationFailure
VS.ERABSetupFailed.InteractionWithOtherProcedure
Monitored class: lte.Cell

Table A-25 ENB Sync And Announce Message Stats

PM counter 3GPP name
VS.SyncMessagesReceived
VS.AnnounceMessagesReceived
VS.SyncMessagesRejected
VS.ErrorredSyncMessagesReceived
Monitored class: lte.ENBEquipment

Table A-26 Enhanced Non-Optimized Redirections To HRPD Via Event B2 Stats

PM counter 3GPP name
VS.NonOptimizedRedirectionToHRPDViaEventB2.SyncModeUeDR
VS.NonOptimizedRedirectionToHRPDViaEventB2.SyncModeUeSR
VS.NonOptimizedRedirectionToHRPDViaEventB2.AsyncModeUeDR
VS.NonOptimizedRedirectionToHRPDViaEventB2.AsyncModeUeSR
VS.NonOptimizedRedirectionToHRPDViaEventB2.NoSysTime
Monitored class: lte.Cell

Table A-27 GBR E-RAB Stats

PM counter 3GPP name
VS.GBRERABSatisfied.Satisfied
VS.GBRERABSatisfied.Unsatisfied
Monitored class: lte.Cell

Table A-28 GEthernet interface Stats

PM counter 3GPP name
VS.IfInOctets
VS.IfInUcastPkts
VS.IfInNucastPkts
VS.IfInDiscards
VS.IfInErrors
VS.IfInUnknownProtos
VS.IfOutOctets
VS.IfOutUcastPkts
VS.IfOutNucastPkts
VS.IfOutDiscards
VS.IfOutErrors
VS.IfInLinkUtilisation.Cum
VS.IfInLinkUtilisation.Min
VS.IfInLinkUtilisation.Max
VS.IfInLinkUtilisation.NbEvt
VS.IfOutLinkUtilisation.Cum
VS.IfOutLinkUtilisation.Max
VS.IfOutLinkUtilisation.Min
VS.IfOutLinkUtilisation.NbEvt
VS.IfInLinkUtilisation
VS.IfOutLinkUtilisation
Monitored class: lte.ENBEquipment

Table A-29 Gap-Assisted Handover Stats

PM counter 3GPP name
VS.OutgoingGapAssistedHOAttempt.IntraLTE

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.OutgoingGapAssistedHOAttempt.InterRAT
VS.OutgoingGapAssistedHOAttempt
VS.OutgoingGapAssistedHOSuccess.IntraLTE
VS.OutgoingGapAssistedHOSuccess.InterRAT
VS.OutgoingGapAssistedHOSuccess
VS.OutgoingGapAssistedHOFailureSum.IntraLTE
VS.OutgoingGapAssistedHOFailureSum.InterRAT
VS.OutgoingGapAssistedHOFailureSum
VS.OutgoingGapAssistedHOAbortSum.IntraLTE
VS.OutgoingGapAssistedHOAbortSum.InterRAT
VS.OutgoingGapAssistedHOAbortSum
Monitored class: lte.Cell

(2 of 2)

Table A-30 HO Cell Selection Stats

PM counter 3GPP name
VS.ReportedCellNotSelected.MobilityNotEnabled
VS.ReportedCellNotSelected.UnknownPCI
VS.ReportedCellNotSelected.CellDisabled
VS.ReportedCellNotSelected.S1HODisabled
VS.ReportedCellNotSelected
Monitored class: lte.Cell

Table A-31 HO Inter-Cell Intra-eNodeB Stats

PM counter 3GPP name
VS.IntraENodeBHOFailure
VS.IntraENodeBHOAbort
VS.IntraENodeBHOFailureSum
VS.IntraENodeBHOFailure.CACFailure
VS.IntraENodeBHOFailure.InternalFailure
VS.IntraENodeBHOFailure.Timeout
VS.IntraENodeBHOFailure.RRCCConnectionReestabOnSourceCell
VS.IntraENodeBHOFailure.RRCCConnectionReestabOnTargetCell
VS.IntraENodeBHOFailure.IntegrityFailure

(1 of 2)

PM counter 3GPP name
VS.IntraENodeBHOFailure.RRCCConnectionReestabOnOtherCell
VS.IntraENodeBHOAbortSum
VS.IntraENodeBHOAbort.S1APResetOrUEContextReleaseCommand
VS.IntraENodeBHOPreparationSuccess
VS.IntraENodeBHOPreparationSuccessScreened.InterFreqSameFrameStructure
VS.IntraENodeBHOPreparationSuccessScreened
VS.IntraENodeBHOFailure.InterFreqCACFailure
VS.IntraENodeBHOFailure.InterFreqInternalFailure
VS.IntraENodeBHOFailure.InterFreqTimeout
VS.IntraENodeBHOFailure.InterFreqRRCCConnectionReestabOnTargetCell
VS.IntraENodeBHOFailure.InterFreqIntegrityFailure
VS.IntraENodeBHOFailure.InterFreqRRCCConnectionReestabOnOtherCell
VS.IntraENodeBHOFailure.InterFreqRRCCConnectionReestabOnSourceCell
VS.IntraENodeBHOAbortScreenedSum.InterFreqSameFrameStructure
VS.IntraENodeBHOAbortScreenedSum
VS.IntraENodeBHOAbort.CsFallback
VS.IntraENodeBHOAbort.EventA1
Monitored class: lte.Cell

(2 of 2)

Table A-32 HO Intra-Cell Stats

PM counter 3GPP name
VS.IntraCellHOAttempt.Rekeying
VS.IntraCellHOAttempt.KeNBRefresh
VS.IntraCellHOSuccess.Rekeying
VS.IntraCellHOSuccess.KeNBRefresh
VS.IntraCellHORekeyingFailure.InternalFailure
VS.IntraCellHORekeyingFailure.Timeout
VS.IntraCellHORekeyingFailure.RRCCConnectionReestablishment
VS.IntraCellHORekeyingFailure.IntegrityFailure
VS.IntraCellHORekeyingFailure.NoSecurityAlgorithm
VS.IntraCellHOKenodeBRefreshFailure.InternalFailure
VS.IntraCellHOKenodeBRefreshFailure.Timeout
VS.IntraCellHOKenodeBRefreshFailure.RRCCConnectionReestablishment
VS.IntraCellHOKenodeBRefreshFailure.IntegrityFailure
VS.IntraCellHOKenodeBRefreshFailure.NoSecurityAlgorithm

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.IntraCellHOAttempt
VS.IntraCellHOSuccess
VS.IntraCellHORekeyingFailure
VS.IntraCellHOKenodeBRefreshFailure
VS.IntraCellHOAttempt.ERABModify
VS.IntraCellHOAttempt.ERABSetup
VS.IntraCellHOSuccess.ERABModify
VS.IntraCellHOSuccess.ERABSetup
VS.IntraCellHOFailureDuringERABModify
VS.IntraCellHOFailureDuringERABSetup
Monitored class: lte.Cell

(2 of 2)

Table A-33 Incoming E-RAB Setup Stats

PM counter 3GPP name
VS.IncomingERABToBeSetupOnIntraLteHO.QCI1
VS.IncomingERABToBeSetupOnIntraLteHO.QCI2
VS.IncomingERABToBeSetupOnIntraLteHO.QCI3
VS.IncomingERABToBeSetupOnIntraLteHO.QCI4
VS.IncomingERABToBeSetupOnIntraLteHO.QCI5
VS.IncomingERABToBeSetupOnIntraLteHO.QCI6
VS.IncomingERABToBeSetupOnIntraLteHO.QCI7
VS.IncomingERABToBeSetupOnIntraLteHO.QCI8
VS.IncomingERABToBeSetupOnIntraLteHO.QCI9
VS.IncomingERABToBeSetupOnIntraLteHO.CustomerQCIs
VS.IncomingERABSetupOnIntraLteHO.QCI1
VS.IncomingERABSetupOnIntraLteHO.QCI2
VS.IncomingERABSetupOnIntraLteHO.QCI3
VS.IncomingERABSetupOnIntraLteHO.QCI4
VS.IncomingERABSetupOnIntraLteHO.QCI5
VS.IncomingERABSetupOnIntraLteHO.QCI6
VS.IncomingERABSetupOnIntraLteHO.QCI7
VS.IncomingERABSetupOnIntraLteHO.QCI8
VS.IncomingERABSetupOnIntraLteHO.QCI9
VS.IncomingERABSetupOnIntraLteHO.CustomerQCIs
VS.IncomingERABSetupOnIRATHO.QCI1

(1 of 2)

PM counter 3GPP name
VS.IncomingERABSetupOnIRATHO.QCI2
VS.IncomingERABSetupOnIRATHO.QCI3
VS.IncomingERABSetupOnIRATHO.QCI4
VS.IncomingERABSetupOnIRATHO.QCI5
VS.IncomingERABSetupOnIRATHO.QCI6
VS.IncomingERABSetupOnIRATHO.QCI7
VS.IncomingERABSetupOnIRATHO.QCI8
VS.IncomingERABSetupOnIRATHO.QCI9
VS.IncomingERABSetupOnIRATHO.CustomerQCI
VS.IncomingERABSetupOnIRATHO
Monitored class: lte.Cell

(2 of 2)

Table A-34 Incoming E-RAB To Be Setup On IRATHO Stats

PM counter 3GPP name
VS.IncomingERABToBeSetupOnIRATHO.QCI1
VS.IncomingERABToBeSetupOnIRATHO.QCI2
VS.IncomingERABToBeSetupOnIRATHO.QCI3
VS.IncomingERABToBeSetupOnIRATHO.QCI4
VS.IncomingERABToBeSetupOnIRATHO.QCI5
VS.IncomingERABToBeSetupOnIRATHO.QCI6
VS.IncomingERABToBeSetupOnIRATHO.QCI7
VS.IncomingERABToBeSetupOnIRATHO.QCI8
VS.IncomingERABToBeSetupOnIRATHO.QCI9
VS.IncomingERABToBeSetupOnIRATHO.CustomerQCI
VS.IncomingERABToBeSetupOnIRATHO
Monitored class: lte.Cell

Table A-35 Incoming HO Inter-Cell Inter-eNodeB via S1 Stats

PM counter 3GPP name
VS.IncomingInterENodeBS1HOAttempt
VS.IncomingInterENodeBS1HOSuccess
VS.IncomingInterENodeBS1HOFailureSum
VS.IncomingInterENodeBS1HOFailure.InterventionOAM

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.IncomingInterENodeBS1HOFailure.CACFailure
VS.IncomingInterENodeBS1HOFailure.InternalFailure
VS.IncomingInterENodeBS1HOFailure.InterEnbS1HTimeout
VS.IncomingInterENodeBS1HOFailure.SecurityAlgoNotCompatible
VS.IncomingInterENodeBS1HOFailure.RRCCConnectionReestablishmentOnTargetCell
VS.IncomingInterENodeBS1HOFailure.IntegrityFailure
VS.IncomingInterENodeBS1HOFailure.RRCCConnectionReestablishmentOnOtherCell
VS.IncomingInterENodeBS1HOFailure.CellNotAvailable
VS.IncomingInterENodeBS1HOAbortSum
VS.IncomingInterENodeBS1HOAbort.S1APUEContextReleaseCommand
VS.IncomingInterENodeBS1HOAttemptScreened.InterFreqSameFrameStructure
VS.IncomingInterENodeBS1HOPreparationSuccessScreened.InterFreqSameFrameStructure
VS.IncomingInterENodeBS1HOSuccessScreened.InterFreqSameFrameStructure
VS.IncomingInterENodeBS1HOFailure.InterFreqInterventionOAM
VS.IncomingInterENodeBS1HOFailure.InterFreqCACFailure
VS.IncomingInterENodeBS1HOFailure.InterFreqInternalFailure
VS.IncomingInterENodeBS1HOFailure.InterFreqInterEnbS1HTimeout
VS.IncomingInterENodeBS1HOFailure.InterFreqSecurityAlgoNotCompatible
VS.IncomingInterENodeBS1HOFailure.InterFreqRRCCConnectionReestablishmentOnTargetCell
VS.IncomingInterENodeBS1HOFailure.InterFreqIntegrityFailure
VS.IncomingInterENodeBS1HOFailure.InterFreqRRCCConnectionReestablishmentOnOtherCell
VS.IncomingInterENodeBS1HOFailure.InterFreqCellNotAvailable
VS.IncomingInterENodeBS1HOFailure.ERABContextAllocationFailure
VS.IncomingInterENodeBS1HOAbortScreenedSum.InterFreqSameFrameStructure
VS.IncomingInterENodeBS1HOFailure
VS.IncomingInterENodeBS1HOAbort
VS.IncomingInterENodeBS1HOAttemptScreened
VS.IncomingInterENodeBS1HOPreparationSuccess
VS.IncomingInterENodeBS1HOPreparationSuccessScreened
VS.IncomingInterENodeBS1HOSuccessScreened
VS.IncomingInterENodeBS1HOAbortScreenedSum
Monitored class: lte.Cell

(2 of 2)

Table A-36 Incoming HO Inter-Cell Inter-eNodeB via X2 Stats

PM counter 3GPP name
VS.IncomingInterENodeBX2HOAttempt
VS.IncomingInterENodeBX2HOSuccess
VS.IncomingInterENodeBX2HOFailureSum
VS.IncomingInterENodeBX2HOFailure.InterventionOAM
VS.IncomingInterENodeBX2HOFailure.CACFailure
VS.IncomingInterENodeBX2HOFailure.InternalFailure
VS.IncomingInterENodeBX2HOFailure.InterEnbHTimeout
VS.IncomingInterENodeBX2HOFailure.PathSwitchFailure
VS.IncomingInterENodeBX2HOFailure.S1PathSwitchTimeout
VS.IncomingInterENodeBX2HOFailure.RRCCConnectionReestablishmentOnTargetCell
VS.IncomingInterENodeBX2HOFailure.S1FaultExternalFailure
VS.IncomingInterENodeBX2HOFailure.IntegrityFailure
VS.IncomingInterENodeBX2HOFailure.SecurityAlgoNotCompatible
VS.IncomingInterENodeBX2HOFailure.RRCCConnectionReestablishmentOnOtherCell
VS.IncomingInterENodeBX2HOFailure.CellNotAvailable
VS.IncomingInterENodeBX2HOAbortSum
VS.IncomingInterENodeBX2HOAbort.X2APHOCancel
VS.IncomingInterENodeBX2HOAttemptScreened.InterFreqSameFrameStructure
VS.IncomingInterENodeBX2HOAttemptScreened
VS.IncomingInterENodeBX2HOPreparationSuccess
VS.IncomingInterENodeBX2HOPreparationSuccessScreened.InterFreqSameFrameStructure
VS.IncomingInterENodeBX2HOPreparationSuccessScreened
VS.IncomingInterENodeBX2HOSuccessScreened.InterFreqSameFrameStructure
VS.IncomingInterENodeBX2HOSuccessScreened
VS.IncomingInterENodeBX2HOFailure.InterFreqInterventionOAM
VS.IncomingInterENodeBX2HOFailure.InterFreqCACFailure
VS.IncomingInterENodeBX2HOFailure.InterFreqInternalFailure
VS.IncomingInterENodeBX2HOFailure.InterFreqInterEnbHTimeout
VS.IncomingInterENodeBX2HOFailure.InterFreqPathSwitchFailure
VS.IncomingInterENodeBX2HOFailure.InterFreqS1PathSwitchTimeout
VS.IncomingInterENodeBX2HOFailure.InterFreqRRCCConnectionReestablishmentOnTargetCell
VS.IncomingInterENodeBX2HOFailure.InterFreqS1FaultExternalFailure
VS.IncomingInterENodeBX2HOFailure.InterFreqIntegrityFailure
VS.IncomingInterENodeBX2HOFailure.InterFreqSecurityAlgoNotCompatible
VS.IncomingInterENodeBX2HOFailure.InterFreqRRCCConnectionReestablishmentOnOtherCell

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.IncomingInterENodeBX2HOFailure.InterFreqCellNotAvailable
VS.IncomingInterENodeBX2HOFailure.ERABContextAllocationFailure
VS.IncomingInterENodeBX2HOAbortScreenedSum.InterFreqSameFrameStructure
VS.IncomingInterENodeBX2HOAbortScreenedSum
VS.IncomingInterENodeBX2HOAbort.X2APReset
Monitored class: lte.Cell

(2 of 2)

Table A-37 Incoming HO Inter-Cell Intra-eNodeB Stats

PM counter 3GPP name
VS.IncomingIntraENodeBHOAttempt
VS.IncomingIntraENodeBHOSuccess
VS.IncomingIntraENodeBHOAttemptScreened.InterFreqSameFrameStructure
VS.IncomingIntraENodeBHOAttemptScreened
VS.IncomingIntraENodeBHOSuccessScreened.InterFreqSameFrameStructure
VS.IncomingIntraENodeBHOSuccessScreened
Monitored class: lte.Cell

Table A-38 Incoming PS Handover From UTRA Stats

PM counter 3GPP name
VS.IncomingPSHOFromUtranAttempt
VS.IncomingPSHOFromUtranPreparationSuccess
VS.IncomingPSHOFromUtranSuccess
VS.IncomingPSHOFromUtranFailureSum
VS.IncomingPSHOFromUtranFailure.InterventionOAM
VS.IncomingPSHOFromUtranFailure.CACFailure
VS.IncomingPSHOFromUtranFailure.InternalFailure
VS.IncomingPSHOFromUtranFailure.interRATIncomingHoTimeout
VS.IncomingPSHOFromUtranFailure.SecurityAlgoNotCompatible
VS.IncomingPSHOFromUtranFailure.RRCCConnectionReestablishmentOnTargetCell
VS.IncomingPSHOFromUtranFailure.IntegrityFailure
VS.IncomingPSHOFromUtranFailure.RRCCConnectionReestablishmentOnOtherCell
VS.IncomingPSHOFromUtranFailure.CellNotAvailable
VS.IncomingPSHOFromUtranFailure

(1 of 2)

PM counter 3GPP name
VS.IncomingPSHOFromUtranAbortSum
VS.IncomingPSHOFromUtranAbort.S1APUEContextReleaseCommand
VS.IncomingPSHOFromUtranAbort
Monitored class: lte.Cell

(2 of 2)

Table A-39 Initial E-RAB Setup Stats

PM counter 3GPP name
VS.InitialERABSetupRequest.QCI1
VS.InitialERABSetupRequest.QCI2
VS.InitialERABSetupRequest.QCI3
VS.InitialERABSetupRequest.QCI4
VS.InitialERABSetupRequest.QCI5
VS.InitialERABSetupRequest.QCI6
VS.InitialERABSetupRequest.QCI7
VS.InitialERABSetupRequest.QCI8
VS.InitialERABSetupRequest.QCI9
VS.InitialERABSetupRequest.CustomerQCIs
VS.InitialERABSetupSuccess.QCI1
VS.InitialERABSetupSuccess.QCI2
VS.InitialERABSetupSuccess.QCI3
VS.InitialERABSetupSuccess.QCI4
VS.InitialERABSetupSuccess.QCI5
VS.InitialERABSetupSuccess.QCI6
VS.InitialERABSetupSuccess.QCI7
VS.InitialERABSetupSuccess.QCI8
VS.InitialERABSetupSuccess.QCI9
VS.InitialERABSetupSuccess.CustomerQCIs
Monitored class: lte.Cell

Table A-40 L1 Connection Stats

PM counter 3GPP name
VS.L1ConnectionRequest
VS.PUCCHCQIPeriodHistogram.LE20ms

(1 of 2)

PM counter 3GPP name
VS.PUCCHCQIPeriodHistogram.40ms
VS.PUCCHCQIPeriodHistogram.80ms
VS.PUCCHCQIPeriodHistogram.GT80ms
VS.PUCCHSRPeriodHistogram.LE20ms
VS.PUCCHSRPeriodHistogram.40ms
VS.PUCCHSRPeriodHistogram.80ms
VS.PUCCHSRPeriodHistogram.GT80ms
VS.PUCCHSRSPeriodHistogram.LE20ms
VS.PUCCHSRSPeriodHistogram.40ms
VS.PUCCHSRSPeriodHistogram.80ms
VS.PUCCHSRSPeriodHistogram.GT80ms
Monitored class: lte.Cell

(2 of 2)

Table A-41 L1 Traffic and throughput MAC-BLER

PM counter 3GPP name
VS.DLInitialMacBLER.LEThreshold1
VS.DLInitialMacBLER.GTThreshold1LEThreshold2
VS.DLInitialMacBLER.GTThreshold2LEThreshold3
VS.DLInitialMacBLER.GTThreshold3LEThreshold4
VS.DLInitialMacBLER.GTThreshold4
VS.DLResidualMacBLER.LEThreshold1
VS.DLResidualMacBLER.GTThreshold1LEThreshold2
VS.DLResidualMacBLER.GTThreshold2LEThreshold3
VS.DLResidualMacBLER.GTThreshold3LEThreshold4
VS.DLResidualMacBLER.GTThreshold4
VS.ULResidualMacBLER.LEThreshold1
VS.ULResidualMacBLER.GTThreshold1LEThreshold2
VS.ULResidualMacBLER.GTThreshold2LEThreshold3
VS.ULResidualMacBLER.GTThreshold3LEThreshold4
VS.ULResidualMacBLER.GTThreshold4
VS.ULInitialMacBLER.LEThreshold1
VS.ULInitialMacBLER.GTThreshold1LEThreshold2
VS.ULInitialMacBLER.GTThreshold2LEThreshold3
VS.ULInitialMacBLER.GTThreshold3LEThreshold4
VS.ULInitialMacBLER.GTThreshold4

(1 of 2)

PM counter 3GPP name
Monitored class: lte.Cell

(2 of 2)

Table A-42 Layer 0 wideband CQI reported in MIMO Stats

PM counter 3GPP name
VS.Layer0MimoWBCqiReported.Cqi0
VS.Layer0MimoWBCqiReported.Cqi1
VS.Layer0MimoWBCqiReported.Cqi2
VS.Layer0MimoWBCqiReported.Cqi3
VS.Layer0MimoWBCqiReported.Cqi4
VS.Layer0MimoWBCqiReported.Cqi5
VS.Layer0MimoWBCqiReported.Cqi6
VS.Layer0MimoWBCqiReported.Cqi7
VS.Layer0MimoWBCqiReported.Cqi8
VS.Layer0MimoWBCqiReported.Cqi9
VS.Layer0MimoWBCqiReported.Cqi10
VS.Layer0MimoWBCqiReported.Cqi11
VS.Layer0MimoWBCqiReported.Cqi12
VS.Layer0MimoWBCqiReported.Cqi13
VS.Layer0MimoWBCqiReported.Cqi14
VS.Layer0MimoWBCqiReported.Cqi15
Monitored class: lte.Cell

Table A-43 Layer 1 wideband CQI reported in MIMO Stats

PM counter 3GPP name
VS.Layer1WBCqiReported.Cqi0
VS.Layer1WBCqiReported.Cqi1
VS.Layer1WBCqiReported.Cqi2
VS.Layer1WBCqiReported.Cqi3
VS.Layer1WBCqiReported.Cqi4
VS.Layer1WBCqiReported.Cqi5
VS.Layer1WBCqiReported.Cqi6
VS.Layer1WBCqiReported.Cqi7
VS.Layer1WBCqiReported.Cqi8

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.Layer1WBCqiReported.Cqi9
VS.Layer1WBCqiReported.Cqi10
VS.Layer1WBCqiReported.Cqi11
VS.Layer1WBCqiReported.Cqi12
VS.Layer1WBCqiReported.Cqi13
VS.Layer1WBCqiReported.Cqi14
VS.Layer1WBCqiReported.Cqi15
Monitored class: lte.Cell

(2 of 2)

Table A-44 Local UE Context Release Stats

PM counter 3GPP name
VS.LocalUEContextRelease.S1APResetMME
VS.LocalUEContextRelease.S1FaultExternalFailure
VS.LocalUEContextRelease.S1APResetENodeB
VS.LocalUEContextRelease.NoContextReleaseCommand
VS.LocalUEContextReleaseSum
Monitored class: lte.Cell

Table A-45 Non-GBR E-RAB RLC Downlink Throughput Stats

PM counter 3GPP name
VS.NonGBRERABRLCThroughputDL.LeRange1
VS.NonGBRERABRLCThroughputDL.GTRange1LeRange2
VS.NonGBRERABRLCThroughputDL.GTRange2LeRange3
VS.NonGBRERABRLCThroughputDL.GTRange3LeRange4
VS.NonGBRERABRLCThroughputDL.GTRange4
Monitored class: lte.Cell

Table A-46 Non-GBR E-RAB RLC Uplink Throughput Stats

PM counter 3GPP name
VS.NonGBRERABRLCThroughputUL.LeRange1
VS.NonGBRERABRLCThroughputUL.GTRange1LeRange2
VS.NonGBRERABRLCThroughputUL.GTRange2LeRange3

(1 of 2)

PM counter 3GPP name
VS.NonGBRERABRlcThroughputUL.GTRange3LeRange4
VS.NonGBRERABRlcThroughputUL.GTRange4
Monitored class: lte.Cell

(2 of 2)

Table A-47 Number Of Bearers Per Cell

PM counter 3GPP name
VS.NbVoIPBearersPerCell
VS.NbGBRBearersPerCell
VS.NbNonGBRBearersPerCell
VS.NbBearersPerCell
Monitored class: lte.Cell

Table A-48 Number Of Bearers Per eNodeB

PM counter 3GPP name
VS.NbVoIPBearersPerENodeB
VS.NbGBRBearersPerENodeB
VS.NbNonGBRBearersPerENodeB
VS.NbBearersPerENodeB
Monitored class: lte.ENBEquipment

Table A-49 OAM VLAN Stats

PM counter 3GPP name
VS.OAMInOctets
VS.OAMInPackets
VS.OAMOutOctets
VS.OAMOutPackets
VS.TelecomInOctets
VS.TelecomInPackets
VS.TelecomOutOctets
VS.TelecomOutPackets
Monitored class: lte.ENBEquipment

Table A-50 Outgoing HO Inter-Cell Inter-eNodeB via S1 Stats

PM counter 3GPP name
VS.OutgoingInterENodeBS1HOAttempt
VS.OutgoingInterENodeBS1HOSuccess
VS.OutgoingInterENodeBS1HOFailureSum
VS.OutgoingInterENodeBS1HOFailure.HOPreparationFailure
VS.OutgoingInterENodeBS1HOFailure.TS1RelocPrepForS1HOTimeout
VS.OutgoingInterENodeBS1HOFailure.RadioLinkFailure
VS.OutgoingInterENodeBS1HOFailure.RRCCConnectionReestablishmentOnSourceCell
VS.OutgoingInterENodeBS1HOFailure.TS1RelocOverallForS1HOTimeout
VS.OutgoingInterENodeBS1HOFailure.RRCCConnectionReestablishmentOnOtherCell
VS.OutgoingInterENodeBS1HOAbortSum
VS.OutgoingInterENodeBS1HOAbort.CascadedHandover
VS.OutgoingInterENodeBS1HOAbort.Other
VS.OutgoingInterENodeBS1HOAttemptScreened.InterFreqSameFrameStructure
VS.OutgoingInterENodeBS1HOPreparationSuccessScreened.InterFreqSameFrameStructure
VS.OutgoingInterENodeBS1HOSuccessScreened.InterFreqSameFrameStructure
VS.OutgoingInterENodeBS1HOFailure.InterFreqHOPreparationFailure
VS.OutgoingInterENodeBS1HOFailure.InterFreqTS1RelocPrepForS1HOTimeout
VS.OutgoingInterENodeBS1HOFailure.InterFreqRadioLinkFailure
VS.OutgoingInterENodeBS1HOFailure.InterFreqRRCCConnectionReestablishmentOnSourceCell
VS.OutgoingInterENodeBS1HOFailure.InterFreqTS1RelocOverallForS1HOTimeout
VS.OutgoingInterENodeBS1HOFailure.InterFreqRRCCConnectionReestablishmentOnOtherCell
VS.OutgoingInterENodeBS1HOAbortScreenedSum.InterFreqSameFrameStructure
VS.OutgoingInterENodeBS1HOAbort.CsFallback
VS.OutgoingInterENodeBS1HOAbort.EventA1
VS.OutgoingInterENodeBS1HOFailure
VS.OutgoingInterENodeBS1HOAbort
VS.OutgoingInterENodeBS1HOAttemptScreened
VS.OutgoingInterENodeBS1HOPreparationSuccess
VS.OutgoingInterENodeBS1HOPreparationSuccessScreened
VS.OutgoingInterENodeBS1HOSuccessScreened
VS.OutgoingInterENodeBS1HOAbortScreenedSum
Monitored class: lte.Cell

Table A-51 Outgoing HO Inter-Cell Inter-eNodeB via X2 Stats

PM counter 3GPP name
VS.OutgoingInterENodeBX2HOAttempt
VS.OutgoingInterENodeBX2HOSuccess
VS.OutgoingInterENodeBX2HOFailure
VS.OutgoingInterENodeBX2HOFailureSum
VS.OutgoingInterENodeBX2HOFailure.HOPreparationFailureOther
VS.OutgoingInterENodeBX2HOFailure.X2PreparationTimeout
VS.OutgoingInterENodeBX2HOFailure.RadioLinkFailure
VS.OutgoingInterENodeBX2HOFailure.RRCCConnectionReestablishmentOnSourceCell
VS.OutgoingInterENodeBX2HOFailure.X2ReleaseTimeout
VS.OutgoingInterENodeBX2HOFailure.RRCCConnectionReestablishmentOnOtherCell
VS.OutgoingInterENodeBX2HOAbortSum
VS.OutgoingInterENodeBX2HOAbort.CascadedHandover
VS.OutgoingInterENodeBX2HOAbort.Other
VS.OutgoingInterENodeBX2HOAttemptScreened.InterFreqSameFrameStructure
VS.OutgoingInterENodeBX2HOPreparationSuccess
VS.OutgoingInterENodeBX2HOPreparationSuccessScreened.InterFreqSameFrameStructure
VS.OutgoingInterENodeBX2HOSuccessScreened.InterFreqSameFrameStructure
VS.OutgoingInterENodeBX2HOFailure.InterFreqHOPreparationFailureOther
VS.OutgoingInterENodeBX2HOFailure.InterFreqX2PreparationTimeout
VS.OutgoingInterENodeBX2HOFailure.InterFreqRRCCConnectionReestablishmentOnSourceCell
VS.OutgoingInterENodeBX2HOFailure.InterFreqX2ReleaseTimeout
VS.OutgoingInterENodeBX2HOFailure.InterFreqRRCCConnectionReestablishmentOnOtherCell
VS.OutgoingInterENodeBX2HOAbortScreenedSum.InterFreqSameFrameStructure
VS.OutgoingInterENodeBX2HOAbortScreenedSum
VS.OutgoingInterENodeBX2HOAbort.CsFallback
VS.OutgoingInterENodeBX2HOAbort.EventA1
VS.OutgoingInterENodeBX2HOAbort.X2APReset
Monitored class: lte.Cell

Table A-52 Outgoing HO Inter-Cell Intra-eNodeB Stats

PM counter 3GPP name
VS.OutgoingIntraENodeBHOAttempt
VS.OutgoingIntraENodeBHOSuccess
VS.OutgoingIntraENodeBHOAttemptScreened.InterFreqSameFrameStructure

(1 of 2)

PM counter 3GPP name
VS.OutgoingIntraENodeBHOAttemptScreened
VS.OutgoingIntraENodeBHOSuccessScreened.InterFreqSameFrameStructure
Monitored class: lte.Cell

(2 of 2)

Table A-53 Outgoing PS Handover To UTRAN FDD

PM counter 3GPP name
VS.OutgoingPSHOToUtraFddAttempt.MeasurementViaEventB2AndThreshold1RSRPThreshold2RSCP
VS.OutgoingPSHOToUtraFddAttempt.MeasurementViaEventB2AndThreshold1RSRPThreshold2EcNO
VS.OutgoingPSHOToUtraFddAttempt.MeasurementViaEventB2AndThreshold1RSRQThreshold2RSCP
VS.OutgoingPSHOToUtraFddAttempt.MeasurementViaEventB2AndThreshold1RSRQThreshold2EcNO
VS.OutgoingPSHOToUtraFddAttempt
VS.OutgoingPSHOToUtraFddPreparationSuccess.MeasurementViaEventB2AndThreshold1RSRPThreshold2RSCP
VS.OutgoingPSHOToUtraFddPreparationSuccess.MeasurementViaEventB2AndThreshold1RSRPThreshold2EcNO
VS.OutgoingPSHOToUtraFddPreparationSuccess.MeasurementViaEventB2AndThreshold1RSRQThreshold2RSCP
VS.OutgoingPSHOToUtraFddPreparationSuccess.MeasurementViaEventB2AndThreshold1RSRQThreshold2EcNO
VS.OutgoingPSHOToUtraFddPreparationSuccess
VS.OutgoingPSHOToUtraFddSuccess.MeasurementViaEventB2AndThreshold1RSRPThreshold2RSCP
VS.OutgoingPSHOToUtraFddSuccess.MeasurementViaEventB2AndThreshold1RSRPThreshold2EcNO
VS.OutgoingPSHOToUtraFddSuccess.MeasurementViaEventB2AndThreshold1RSRQThreshold2RSCP
VS.OutgoingPSHOToUtraFddSuccess.MeasurementViaEventB2AndThreshold1RSRQThreshold2EcNO
VS.OutgoingPSHOToUtraFddSuccess
Monitored class: lte.Cell

Table A-54 Outgoing PS Handover To UTRAN FDD Failure And Abort Stats

PM counter 3GPP name
VS.OutgoingPSHOToUtraFddFailureSum
VS.OutgoingPSHOToUtraFddFailure.HOPreparationFailure
VS.OutgoingPSHOToUtraFddFailure.TS1RelocPrepForPSHOToUtraTimeout
VS.OutgoingPSHOToUtraFddFailure.RadioLinkFailure
VS.OutgoingPSHOToUtraFddFailure.RRCCONNECTIONReestablishmentOnSourceCell
VS.OutgoingPSHOToUtraFddFailure.RRCCONNECTIONReestablishmentOnOtherCell
VS.OutgoingPSHOToUtraFddFailure.TS1RelocOverallForPSHOToUtraTimeout
VS.OutgoingPSHOToUtraFddFailure

(1 of 2)

PM counter 3GPP name
VS.OutgoingPSHOTOltraFddAbortSum
VS.OutgoingPSHOTOltraFddAbort.S1APUEContextReleaseCommand
VS.OutgoingPSHOTOltraFddAbort.CascadedHandover
VS.OutgoingPSHOTOltraFddAbort.Other
VS.OutgoingPSHOTOltraFddAbort.CsFallback
VS.OutgoingPSHOTOltraFddAbort.EventA1
VS.OutgoingPSHOTOltraFddAbort
Monitored class: lte.Cell

(2 of 2)

Table A-55 Outgoing PS Handover To UTRAN TDD

PM counter 3GPP name
VS.OutgoingPSHOTOltraTddAttempt.PSHOViaEventB2AndThreshold1RSRP
VS.OutgoingPSHOTOltraTddAttempt.PSHOViaEventB2AndThreshold1RSRQ
VS.OutgoingPSHOTOltraTddAttempt
VS.OutgoingPSHOTOltraTddSuccess.PSHOViaEventB2AndThreshold1RSRP
VS.OutgoingPSHOTOltraTddSuccess.PSHOViaEventB2AndThreshold1RSRQ
VS.OutgoingPSHOTOltraTddSuccess
VS.OutgoingPSHOTOltraTddFailureSum
VS.OutgoingPSHOTOltraTddFailure.HOPreparationFailure
VS.OutgoingPSHOTOltraTddFailure.TS1RelocPrepForPSHOTOltraTimeout
VS.OutgoingPSHOTOltraTddFailure.RadioLinkFailure
VS.OutgoingPSHOTOltraTddFailure.RRCCConnectionReestablishmentOnSourceCell
VS.OutgoingPSHOTOltraTddFailure.RRCCConnectionReestablishmentOnOtherCell
VS.OutgoingPSHOTOltraTddFailure.TS1RelocOverallForPSHOTOltraTimeout
VS.OutgoingPSHOTOltraTddFailure
VS.OutgoingPSHOTOltraTddAbortSum
VS.OutgoingPSHOTOltraTddAbort.S1APUEContextReleaseCommand
VS.OutgoingPSHOTOltraTddAbort.CascadedHandover
VS.OutgoingPSHOTOltraTddAbort.Other
VS.OutgoingPSHOTOltraTddAbort
Monitored class: lte.Cell

Table A-56 PRBs Pool Overload Stats

PM counter 3GPP name
VS.DLPRBsPoolOverloadScreened.ModemReport
VS.DLPRBsPoolOverloadScreened.CAC
VS.DLPRBsPoolOverloadScreened.NbEvt
VS.DLPRBsPoolOverloadScreened.Cum
VS.DLPRBsPoolOverloadScreened.Max
VS.DLPRBsPoolOverloadScreened.Min
VS.ULPRBsPoolOverloadScreened.ModemReport
VS.ULPRBsPoolOverloadScreened.CAC
VS.ULPRBsPoolOverloadScreened.NbEvt
VS.ULPRBsPoolOverloadScreened.Cum
VS.ULPRBsPoolOverloadScreened.Max
VS.ULPRBsPoolOverloadScreened.Min
VS.DLPRBsPoolOverloadScreened
VS.ULPRBsPoolOverloadScreened
Monitored class: lte.Cell

Table A-57 PS Handover to UTRAN FDD Stats

PM counter 3GPP name
VS.OutgoingBlindPSHOToUtraFddAttempt
VS.OutgoingBlindPSHOToUtraFddAttempt.BlindViaEventA2AndThreshold1RSRP
VS.OutgoingBlindPSHOToUtraFddAttempt.BlindViaEventA2AndThreshold1RSRQ
VS.OutgoingBlindPSHOToUtraFddSuccess
VS.OutgoingBlindPSHOToUtraFddSuccess.BlindViaEventA2AndThreshold1RSRQ
VS.OutgoingBlindPSHOToUtraFddSuccess.BlindViaEventA2AndThreshold1RSRP
VS.OutgoingBlindPSHOToUtraFddFailure
VS.OutgoingBlindPSHOToUtraFddFailure.HOPreparationFailure
VS.OutgoingBlindPSHOToUtraFddFailure.TS1RelocOveralForPSHOToUtraTimeout
VS.OutgoingBlindPSHOToUtraFddFailure.RadioLinkFailure
VS.OutgoingBlindPSHOToUtraFddFailure.TS1RelocPrepForPSHOToUtraTimeout
VS.OutgoingBlindPSHOToUtraFddFailure.RRCCConnectionReestablishmentOnSourceCell
VS.OutgoingBlindPSHOToUtraFddFailureSum
VS.OutgoingBlindPSHOToUtraFddFailure.RRCCConnectionReestablishmentOnOtherCell
VS.OutgoingBlindPSHOToUtraFddAbort
VS.OutgoingBlindPSHOToUtraFddAbortSum

(1 of 2)

PM counter 3GPP name
VS.OutgoingBlindPSHOTOltraFddAbort.CascadedHandover
VS.OutgoingBlindPSHOTOltraFddAbort.S1APUEContextReleaseCommand
VS.OutgoingBlindPSHOTOltraFddAbort.Other
Monitored class: lte.ENBEquipment

(2 of 2)

Table A-58 PS Handover to UTRAN TDD Stats

PM counter 3GPP name
VS.OutgoingBlindPSHOTOltraTddAttempt.BlindViaEventA2AndThreshold1RSRP
VS.OutgoingBlindPSHOTOltraTddAttempt.BlindViaEventA2AndThreshold1RSRQ
VS.OutgoingBlindPSHOTOltraTddAttempt
VS.OutgoingBlindPSHOTOltraTddSuccess.BlindViaEventA2AndThreshold1RSRP
VS.OutgoingBlindPSHOTOltraTddSuccess.BlindViaEventA2AndThreshold1RSRQ
VS.OutgoingBlindPSHOTOltraTddSuccess
VS.OutgoingBlindPSHOTOltraTddFailureSum
VS.OutgoingBlindPSHOTOltraTddFailure.HOPreparationFailure
VS.OutgoingBlindPSHOTOltraTddFailure.TS1RelocPrepForPSHOTOltraTimeout
VS.OutgoingBlindPSHOTOltraTddFailure.RadioLinkFailure
VS.OutgoingBlindPSHOTOltraTddFailure.RRCCConnectionReestablishmentOnSourceCell
VS.OutgoingBlindPSHOTOltraTddFailure.RRCCConnectionReestablishmentOnOtherCell
VS.OutgoingBlindPSHOTOltraTddFailure.TS1RelocOverallForPSHOTOltraTimeout
VS.OutgoingBlindPSHOTOltraTddFailure
VS.OutgoingBlindPSHOTOltraTddAbortSum
VS.OutgoingBlindPSHOTOltraTddAbort.S1APUEContextReleaseCommand
VS.OutgoingBlindPSHOTOltraTddAbort.CascadedHandover
VS.OutgoingBlindPSHOTOltraTddAbort.Other
VS.OutgoingBlindPSHOTOltraTddAbort
Monitored class: lte.ENBEquipment

Table A-59 Paging Attempt Stats

PM counter 3GPP name
VS.S1PageAttemptsFromMMEs
VS.S1PageAttemptsDiscarded.InterventionOAM
VS.S1PageAttemptsDiscarded.CellNotAvailableInternalFailure

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.S1PageAttemptsDiscarded
Monitored class: lte.ENBEquipment

(2 of 2)

Table A-60 Power Headroom Stats

PM counter 3GPP name
VS.ULPHnormalized.LeRange1
VS.ULPHnormalized.GTRange1LeRange2
VS.ULPHnormalized.GTRange2LeRange3
VS.ULPHnormalized.GTRange3LeRange4
VS.ULPHnormalized.GTRange4
Monitored class: lte.Cell

Table A-61 RACH

PM counter 3GPP name
VS.ContentionBasedRandomAccessPreamble
VS.ContentionFreeRandomAccessPreamble
VS.ContentionBasedRandomAccessResponse
VS.ContentionFreeRandomAccessResponse
VS.ContentionResolution
Monitored class: lte.Cell

Table A-62 RRC Connection Release Due To MME Overload

PM counter 3GPP name
VS.RrcConnectionReleaseDueToMMEOverload.MoData
VS.RrcConnectionReleaseDueToMMEOverload.MoDataMoSignalling
VS.RrcConnectionReleaseDueToMMEOverload.NonEmergencyNonMtAccess
VS.RrcConnectionReleaseDueToMMEOverload
Monitored class: lte.Cell

Table A-63 RRC Connection Setup Stats

PM counter 3GPP name
VS.RrcConnectionRequest.EmergencyCallAttempts
VS.RrcConnectionRequest.HighPriorityAccessAttempts
VS.RrcConnectionRequest.PageResponsesReceived
VS.RrcConnectionRequest.MobileOriginatedSignalling
VS.RrcConnectionRequest.MobileOriginatedUserBearer
VS.RrcConnectionRequest.Other
VS.RrcConnectionSuccessSum
VS.RrcConnectionFailureSum
VS.RrcConnectionFailure.CACFailure
VS.RrcConnectionFailure.NoResponseFromUE
VS.RrcConnectionFailure.S1FaultExternalFailure
VS.RrcConnectionFailure.InterventionOAM
VS.RrcConnectionFailure.MoData
VS.RrcConnectionFailure.MoDataMoSignalling
VS.RrcConnectionFailure.NonEmergencyNonMtAccess
VS.RrcConnectionRequest
VS.RrcConnectionFailure
Monitored class: lte.Cell

Table A-64 RRC Connection Stats

PM counter 3GPP name
VS.NbUeRrcConnected.Cum
VS.NbUeRrcConnected.Max
VS.NbUeRrcConnected.Min
VS.NbUeRrcConnected.NbEvt
VS.NbUeRrcConnected
Monitored class: lte.Cell

Table A-65 RRC Reestablishment Setup Stats

PM counter 3GPP name
VS.RrcConnectionReestablishmentRequest
VS.RrcConnectionReestablishmentSuccess.OnTargetCellDuringIntraENodeBHO

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.RrcConnectionReestablishmentSuccess.OnTargetCellDuringInterENodeBX2HO
VS.RrcConnectionReestablishmentSuccess.OnTargetCellDuringInterENodeBS1HO
VS.RrcConnectionReestablishmentSuccess.OnOtherCellDuringHO
VS.RrcConnectionReestablishmentSuccess.OnNotServingCellNotDuringHO
VS.RrcConnectionReestablishmentSuccess.Other
VS.RrcConnectionReestablishmentFailureSum
VS.RrcConnectionReestablishmentFailure
VS.RrcConnectionReestablishmentFailure.ReestablishmentNotAllowed
VS.RrcConnectionReestablishmentFailure.ReestabUEIdUnknown
VS.RrcConnectionReestablishmentFailure.RrcConnectionReestabTimeout
VS.RrcConnectionReestablishmentFailure.RrcConnectionReconfigTimeout
VS.RrcConnectionReestablishmentFailure.NewRrcConnectionReestabRequest
VS.RrcConnectionReestablishmentFailure.RadioLinkFailure
VS.RrcConnectionReestablishmentFailure.ShortMACMismatch
VS.RrcConnectionReestablishmentFailure.S1FaultExternalFailure
VS.RrcConnectionReestablishmentFailure.InterventionOAM
VS.RrcConnectionReestablishmentFailure.CACFailure
VS.RrcConnectionReestablishmentFailure.IntegrityFailure
VS.RrcConnectionReestablishmentSuccess.OnTargetCellDuringIntraENodeBInterFreqSameFrameStructureHO
VS.RrcConnectionReestablishmentSuccess.OnTargetCellDuringInterENodeBInterFreqSameFrameStructureX2HO
VS.RrcConnectionReestablishmentSuccess.OnTargetCellDuringInterENodeBInterFreqSameFrameStructureS1HO
VS.RrcConnectionReestablishmentSuccess
VS.RrcConnectionReestablishmentSuccess.OnTargetCellDuringIncomingPSHO
Monitored class: lte.Cell

(2 of 2)

Table A-66 Radio Link Stats

PM counter 3GPP name
VS.RadioLinkFailureSum
VS.RadioLinkFailure
VS.RadioLinkFailure.MaxNbRlcRetransReached
VS.RadioLinkFailure.LossOfUuL1Synchron
Monitored class: lte.Cell

Table A-67 Redirection To HRPD Stats

PM counter 3GPP name
VS.NonOptimizedRedirectionToHRPDViaEventA2
Monitored class: lte.Cell

Table A-68 Redirection To Inter-Frequency Intra-FDD or TDD Stats

PM counter 3GPP name
VS.RedirectionToInterFrequencyIntraFDDorTDD
VS.RedirectionToInterFrequencyIntraFDDorTDD.BlindViaEventA2AndThreshold1RSRP
VS.RedirectionToInterFrequencyIntraFDDorTDD.BlindViaEventA2AndThreshold1RSRQ
Monitored class: lte.Cell

Table A-69 Redirection To Inter-Frequency Same Frame Structure Stats

PM counter 3GPP name
VS.RedirectionToInterFrequencySameFrameStructure.BlindViaEventA2AndThreshold1RSRP
VS.RedirectionToInterFrequencySameFrameStructure.BlindViaEventA2AndThreshold1RSRQ
VS.RedirectionToInterFrequencySameFrameStructure.EventA3OrA5
Monitored class: lte.Cell

Table A-70 Redirection to GERAN Stats

PM counter 3GPP name
VS.RedirectionToGeran.MeasurementViaEventB2AndThreshold1RSRPThreshold2GERAN
VS.RedirectionToGeran.MeasurementViaEventB2AndThreshold1RSRQThreshold2GERAN
VS.RedirectionToGeran.BlindViaEventA2AndThreshold1RSRP
VS.RedirectionToGeran.BlindViaEventA2AndThreshold1RSRQ
VS.RedirectionToGeran.CsFallbackTriggered
Monitored class: lte.Cell

Table A-71 Redirection to UTRAN FDD Stats

PM counter 3GPP name
VS.RedirectionToUtraFdd.MeasurementViaEventB2AndThreshold1RSRPThreshold2RSCP

(1 of 2)

PM counter 3GPP name
VS.RedirectionToUtraFdd.MeasurementViaEventB2AndThreshold1RSRPThreshold2EcNO
VS.RedirectionToUtraFdd.MeasurementViaEventB2AndThreshold1RSRQThreshold2RSCP
VS.RedirectionToUtraFdd.MeasurementViaEventB2AndThreshold1RSRQThreshold2EcNO
VS.RedirectionToUtraFdd.BlindViaEventA2AndThreshold1RSRP
VS.RedirectionToUtraFdd.BlindViaEventA2AndThreshold1RSRQ
VS.RedirectionToUtraFdd.CsFallbackTriggered
Monitored class: lte.Cell

(2 of 2)

Table A-72 Redirection to UTRAN TDD Stats

PM counter 3GPP name
VS.RedirectionToUtraTdd.BlindViaEventA2AndThreshold1RSRP
VS.RedirectionToUtraTdd.BlindViaEventA2AndThreshold1RSRQ
VS.RedirectionToUtraTdd.MeasurementViaEventB2AndThreshold1RSRPThreshold2RSCP
VS.RedirectionToUtraTdd.MeasurementViaEventB2AndThreshold1RSRQThreshold2RSCP
Monitored class: lte.Cell

Table A-73 S1 Error Indication By MME Stats

PM counter 3GPP name
VS.S1ErrorIndicationByMME.UnknownOrAlreadyAllocatedMMEUES1apId
VS.S1ErrorIndicationByMME.UnknownOrAlreadyAllocatedeNodeBUES1apId
VS.S1ErrorIndicationByMME.UnknownOrAlreadyAllocatedPairOfUES1apId
VS.S1ErrorIndicationByMME.ProtocolError
VS.S1ErrorIndicationByMME.Other
VS.S1ErrorIndicationByMME
Monitored class: lte.ENBEquipment

Table A-74 S1 Error Indication By eNodeB Stats

PM counter 3GPP name
VS.S1ErrorIndicationByENodeB.UnknownOrAlreadyAllocatedMMEUES1apId
VS.S1ErrorIndicationByENodeB.UnknownOrAlreadyAllocatedeNodeBUES1apId
VS.S1ErrorIndicationByENodeB.UnknownOrAlreadyAllocatedPairOfUES1apId
VS.S1ErrorIndicationByENodeB.ProtocolError

(1 of 2)

PM counter 3GPP name
VS.S1ErrorIndicationByENodeB.Other
VS.S1ErrorIndicationByENodeB
Monitored class: lte.ENBEquipment

(2 of 2)

Table A-75 S1 SCTP Traffic Stats

PM counter 3GPP name
VS.S1SctpInOctets
VS.S1SctpInPackets
VS.S1SctpOutOctets
VS.S1SctpOutPackets
Monitored class: lte.MmeAccess

Table A-76 S1 Setup Stats

PM counter 3GPP name
VS.InitialUEMessage
VS.FirstDLNasTransport
VS.UEContextSetupRequest
VS.UEContextSetupRequest.WithoutPreviousDLNasTransport
VS.UEContextSetupRequest.AfterDLNasTransport
VS.S1ConnectionEstablishmentFailure
VS.S1ConnectionEstablishmentFailure.Timeout
Monitored class: lte.Cell

Table A-77 SCTP Association Stats

PM counter 3GPP name
VS.SctpAssociationEstablishment
VS.SctpAssociationFailure
Monitored class: lte.ENBEquipment

Table A-78 Throughput On S1 interfaces Stats

PM counter 3GPP name
VS.S1DLThroughput
VS.S1DLThroughput.Cum
VS.S1DLThroughput.Max
VS.S1DLThroughput.Min
VS.S1DLThroughput.NbEvt
VS.S1ULThroughput
VS.S1ULThroughput.Cum
VS.S1ULThroughput.Max
VS.S1ULThroughput.Min
VS.S1ULThroughput.NbEvt
Monitored class: lte.ENBEquipment

Table A-79 Throughput On X2 interfaces Stats

PM counter 3GPP name
VS.X2ReceivedThroughput.Cum
VS.X2ReceivedThroughput.Max
VS.X2ReceivedThroughput.Min
VS.X2ReceivedThroughput.NbEvt
VS.X2SentThroughput.Cum
VS.X2SentThroughput.Max
VS.X2SentThroughput.Min
VS.X2SentThroughput.NbEvt
Monitored class: lte.ENBEquipment

Table A-80 Traffic On S1 interfaces Stats

PM counter 3GPP name
VS.S1DLPacketsPerSecond
VS.S1ULPacketsPerSecond
VS.S1DLPackets
VS.S1ULPackets
Monitored class: lte.ENBEquipment

Table A-81 Traffic On X2 interfaces Stats

PM counter 3GPP name
VS.X2ReceivedPacketsPerSecond
VS.X2SentPacketsPerSecond
VS.X2ReceivedPackets
VS.X2SentPackets
Monitored class: lte.ENBEquipment

Table A-82 Transport Block Stats

PM counter 3GPP name
VS.TotalCountOfULTransportBlocks
VS.TotalCountOfErrorULTransportBlocks
VS.TotalCountOfDLTransportBlocks
VS.TotalCountOfErrorDLTransportBlocks
Monitored class: lte.Cell

Table A-83 UE Context Modification Stats

PM counter 3GPP name
VS.UContextmodificationAttempt
VS.UContextmodificationSuccess
VS.UContextModificationFailure.FailureInTheRadioInterfaceProcedure
VS.UContextModificationFailure.EncryptionAndOrIntegrityProtectionAlgorithmsNotSupported
VS.UContextModificationFailure.X2HandoverTriggered
VS.UContextModificationFailure.S1IntraSystemHandoverTriggered
VS.UContextModificationFailure.S1InterSystemHandoverTriggered
VS.UContextModificationFailure.AbstractSyntaxError
VS.UContextModificationFailure.Unspecified
VS.UContextModificationFailure
Monitored class: lte.Cell

Table A-84 UE Context Release Command Stats

PM counter 3GPP name
VS.UContextReleaseCommandSum
VS.UContextReleaseCommand.ResponseToReleaseRequest
VS.UContextReleaseCommand.NormalRelease
VS.UContextReleaseCommand.AuthenticationFailure
VS.UContextReleaseCommand.Detach
VS.UContextReleaseCommand.SuccessfulHandover
Monitored class: lte.Cell

Table A-85 UE Context Release Request Stats

PM counter 3GPP name
VS.UContextReleaseRequestSum
VS.UContextReleaseRequest
VS.UContextReleaseRequest.UserInactivity
VS.UContextReleaseRequest.RadioLinkFailure
VS.UContextReleaseRequest.InternalFailure
VS.UContextReleaseRequest.NoInitialContextSetupRequest
VS.UContextReleaseRequest.IntegrityFailure
VS.UContextReleaseRequest.InterRATRedirection
VS.UContextReleaseRequest.SecurityAlgoNotCompatible
VS.UContextReleaseRequest.RadioInterfaceFailure
VS.UContextReleaseRequest.TS1RelocOverallForS1HOTimeout
VS.UContextReleaseRequest.X2ReleaseTimeout
VS.UContextReleaseRequest.TS1RelocOverallForPSHOToUtraTimeout
VS.UContextReleaseRequest.InterFreqRedirection
VS.UContextReleaseCommandSum
VS.UContextReleaseCommand.ResponseToReleaseRequest
VS.UContextReleaseCommand.NormalRelease
VS.UContextReleaseCommand.AuthenticationFailure
VS.UContextReleaseCommand.Detach
VS.UContextReleaseCommand.SuccessfulHandover
VS.UContextReleaseRequest.TMobilityFromEutraCCOTimeoutWithNACC
VS.UContextReleaseRequest.TMobilityFromEutraCCOTimeoutWithoutNACC
VS.UContextReleaseRequest.CsFallbackNotPossible
Monitored class: lte.Cell

Table A-86 UE Context Setup Stats

PM counter 3GPP name
VS.InitialContextSetupSuccess
VS.InitialContextSetupSuccess.WithoutPreviousDLNASTransport
VS.InitialContextSetupSuccess.AfterDLNASTransport
VS.InitialContextSetupFailedSum
VS.InitialContextSetupFailed.CACFailure
VS.InitialContextSetupFailed.InternalFailure
VS.InitialContextSetupFailed.Timeout
VS.InitialContextSetupFailed.RRCCConnectionReestablishment
VS.InitialContextSetupFailed.SecurityActivationFailure
VS.InitialContextSetupFailed.IntegrityFailure
VS.InitialContextSetupFailed.SecurityAlgoNotCompatible
VS.InitialContextSetupFailed.ERABContextAllocationFailure
VS.InitialContextSetupFailed.CsFallbackNotPossible
Monitored class: lte.Cell

Table A-87 UE scheduled per TTI Stats

PM counter 3GPP name
VS.NbUeScheduledPerDLTTI.Cum
VS.NbUeScheduledPerDLTTI.Max
VS.NbUeScheduledPerDLTTI.Min
VS.NbUeScheduledPerDLTTI.NbEvt
VS.NbUeScheduledPerULTTI
VS.NbUeScheduledPerDLTTI
Monitored class: lte.Cell

Table A-88 UL PRB Usage Stats

PM counter 3GPP name
VS.ULTotalPRBUsage
VS.ULPRBUsagePerTrafficClass.VoIP
VS.ULPRBUsagePerTrafficClass.GBR
VS.ULPRBUsagePerTrafficClass.NonGBR
VS.ULPRBUsagePerTrafficClass

(1 of 2)

PM counter 3GPP name
Monitored class: lte.Cell

(2 of 2)

Table A-89 Uplink Cell PDCP SDU Volume Stats

PM counter 3GPP name
VS.DRBPdcpSduKbytesUL.VoIP
VS.DRBPdcpSduKbytesUL.OtherGBR
VS.DRBPdcpSduKbytesUL.NonGBR
VS.DRBPdcpSduKbytesUL
VS.DRBPdcpSduBitRateUL
Monitored class: lte.Cell

Table A-90 Uplink Grants per TTI Stats

PM counter 3GPP name
VS.ULGrant.0Grant
VS.ULGrant.1Grant
VS.ULGrant.2Grants
VS.ULGrant.3Grants
VS.ULGrant.4Grants
VS.ULGrant.5Grants
VS.ULGrant.6orMoreGrants
Monitored class: lte.Cell

Table A-91 Uplink L2 Traffic and Throughput Stats

PM counter 3GPP name
VS.ULRlcPduKbytes.VoIP
VS.ULRlcPduKbytes.GBR
VS.ULRlcPduKbytes.NonGBR
VS.ULRlcPduReceived.VoIP
VS.ULRlcPduReceived.GBR
VS.ULRlcPduReceived.NonGBR
Monitored class: lte.Cell

Table A-92 Uplink Noise For PRB1

PM counter 3GPP name
VS.ULNoise.LeRg1PRB1
VS.ULNoise.GtRg1LeRg2PRB1
VS.ULNoise.GtRg2LeRg3PRB1
VS.ULNoise.GtRg3LeRg4PRB1
VS.ULNoise.GtRg4PRB1
VS.LeRg1PRBg1
VS.GtRg1LeRg2PRBg1
VS.GtRg2LeRg3PRBg1
VS.GtRg3LeRg4PRBg1
VS.GtRg4PRBg1
Monitored class: lte.Cell

Table A-93 Uplink Noise For PRB10

PM counter 3GPP name
VS.ULNoise.LeRg1PRB10
VS.ULNoise.GtRg1LeRg2PRB10
VS.ULNoise.GtRg2LeRg3PRB10
VS.ULNoise.GtRg3LeRg4PRB10
VS.ULNoise.GtRg4PRB10
VS.ULNoisePerPRBGroup.LeRg1PRBg10
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg10
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg10
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg10
VS.ULNoisePerPRBGroup.GtRg4PRBg10
Monitored class: lte.Cell

Table A-94 Uplink Noise For PRB100

PM counter 3GPP name
VS.ULNoise.LeRg1PRB100
VS.ULNoise.GtRg1LeRg2PRB100
VS.ULNoise.GtRg2LeRg3PRB100
VS.ULNoise.GtRg3LeRg4PRB100

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.ULNoise.GtRg4PRB100
Monitored class: lte.Cell

(2 of 2)

Table A-95 Uplink Noise For PRB11

PM counter 3GPP name
VS.ULNoise.LeRg1PRB11
VS.ULNoise.GtRg1LeRg2PRB11
VS.ULNoise.GtRg2LeRg3PRB11
VS.ULNoise.GtRg3LeRg4PRB11
VS.ULNoise.GtRg4PRB11
VS.ULNoisePerPRBGroup.LeRg1PRBg11
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg11
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg11
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg11
VS.ULNoisePerPRBGroup.GtRg4PRBg11
Monitored class: lte.Cell

Table A-96 Uplink Noise For PRB12

PM counter 3GPP name
VS.ULNoise.LeRg1PRB12
VS.ULNoise.GtRg1LeRg2PRB12
VS.ULNoise.GtRg2LeRg3PRB12
VS.ULNoise.GtRg3LeRg4PRB12
VS.ULNoise.GtRg4PRB12
VS.ULNoisePerPRBGroup.LeRg1PRBg12
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg12
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg12
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg12
VS.ULNoisePerPRBGroup.GtRg4PRBg12
Monitored class: lte.Cell

Table A-97 Uplink Noise For PRB13

PM counter 3GPP name
VS.ULNoise.LeRg1PRB13
VS.ULNoise.GtRg1LeRg2PRB13
VS.ULNoise.GtRg2LeRg3PRB13
VS.ULNoise.GtRg3LeRg4PRB13
VS.ULNoise.GtRg4PRB13
VS.ULNoisePerPRBGroup.LeRg1PRBg13
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg13
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg13
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg13
VS.ULNoisePerPRBGroup.GtRg4PRBg13
Monitored class: lte.Cell

Table A-98 Uplink Noise For PRB14

PM counter 3GPP name
VS.ULNoise.LeRg1PRB14
VS.ULNoise.GtRg1LeRg2PRB14
VS.ULNoise.GtRg2LeRg3PRB14
VS.ULNoise.GtRg3LeRg4PRB14
VS.ULNoise.GtRg4PRB14
VS.ULNoisePerPRBGroup.LeRg1PRBg14
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg14
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg14
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg14
VS.ULNoisePerPRBGroup.GtRg4PRBg14
Monitored class: lte.Cell

Table A-99 Uplink Noise For PRB15

PM counter 3GPP name
VS.ULNoise.LeRg1PRB15
VS.ULNoise.GtRg1LeRg2PRB15
VS.ULNoise.GtRg2LeRg3PRB15
VS.ULNoise.GtRg3LeRg4PRB15

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.ULNoise.GtRg4PRB15
VS.ULNoisePerPRBGroup.LeRg1PRBg15
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg15
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg15
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg15
VS.ULNoisePerPRBGroup.GtRg4PRBg15
Monitored class: lte.Cell

(2 of 2)

Table A-100 Uplink Noise For PRB16

PM counter 3GPP name
VS.ULNoise.LeRg1PRB16
VS.ULNoise.GtRg1LeRg2PRB16
VS.ULNoise.GtRg2LeRg3PRB16
VS.ULNoise.GtRg3LeRg4PRB16
VS.ULNoise.GtRg4PRB16
VS.ULNoisePerPRBGroup.LeRg1PRBg16
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg16
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg16
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg16
VS.ULNoisePerPRBGroup.GtRg4PRBg16
Monitored class: lte.Cell

Table A-101 Uplink Noise For PRB17

PM counter 3GPP name
VS.ULNoise.LeRg1PRB17
VS.ULNoise.GtRg1LeRg2PRB17
VS.ULNoise.GtRg2LeRg3PRB17
VS.ULNoise.GtRg3LeRg4PRB17
VS.ULNoise.GtRg4PRB17
VS.ULNoisePerPRBGroup.LeRg1PRBg17
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg17
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg17
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg17

(1 of 2)

PM counter 3GPP name
VS.ULNoisePerPRBGroup.GtRg4PRBg17
Monitored class: lte.Cell

(2 of 2)

Table A-102 Uplink Noise For PRB18

PM counter 3GPP name
VS.ULNoise.LeRg1PRB18
VS.ULNoise.GtRg1LeRg2PRB18
VS.ULNoise.GtRg2LeRg3PRB18
VS.ULNoise.GtRg3LeRg4PRB18
VS.ULNoise.GtRg4PRB18
Monitored class: lte.Cell

Table A-103 Uplink Noise For PRB19

PM counter 3GPP name
VS.ULNoise.LeRg1PRB19
VS.ULNoise.GtRg1LeRg2PRB19
VS.ULNoise.GtRg2LeRg3PRB19
VS.ULNoise.GtRg3LeRg4PRB19
VS.ULNoise.GtRg4PRB19
VS.ULNoisePerPRBGroup.LeRg1PRBg19
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg19
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg19
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg19
VS.ULNoisePerPRBGroup.GtRg4PRBg19
Monitored class: lte.Cell

Table A-104 Uplink Noise For PRB2

PM counter 3GPP name
VS.ULNoise.LeRg1PRB2
VS.ULNoise.GtRg1LeRg2PRB2
VS.ULNoise.GtRg2LeRg3PRB2
VS.ULNoise.GtRg3LeRg4PRB2

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.ULNoise.GtRg4PRB2
VS.LeRg1PRBg2
VS.GtRg1LeRg2PRBg2
VS.GtRg2LeRg3PRBg2
VS.GtRg3LeRg4PRBg2
VS.GtRg4PRBg2
Monitored class: lte.Cell

(2 of 2)

Table A-105 Uplink Noise For PRB20

PM counter 3GPP name
VS.ULNoise.LeRg1PRB20
VS.ULNoise.GtRg1LeRg2PRB20
VS.ULNoise.GtRg2LeRg3PRB20
VS.ULNoise.GtRg3LeRg4PRB20
VS.ULNoise.GtRg4PRB20
VS.ULNoisePerPRBGroup.LeRg1PRBg20
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg20
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg20
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg20
VS.ULNoisePerPRBGroup.GtRg4PRBg20
Monitored class: lte.Cell

Table A-106 Uplink Noise For PRB21

PM counter 3GPP name
VS.ULNoise.LeRg1PRB21
VS.ULNoise.GtRg1LeRg2PRB21
VS.ULNoise.GtRg2LeRg3PRB21
VS.ULNoise.GtRg3LeRg4PRB21
VS.ULNoise.GtRg4PRB21
VS.ULNoisePerPRBGroup.LeRg1PRBg21
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg21
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg21
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg21

(1 of 2)

PM counter 3GPP name
VS.ULNoisePerPRBGroup.GtRg4PRBg21
Monitored class: lte.Cell

(2 of 2)

Table A-107 Uplink Noise For PRB22

PM counter 3GPP name
VS.ULNoise.LeRg1PRB22
VS.ULNoise.GtRg1LeRg2PRB22
VS.ULNoise.GtRg2LeRg3PRB22
VS.ULNoise.GtRg3LeRg4PRB22
VS.ULNoise.GtRg4PRB22
VS.ULNoisePerPRBGroup.LeRg1PRBg22
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg22
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg22
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg22
VS.ULNoisePerPRBGroup.GtRg4PRBg22
Monitored class: lte.Cell

Table A-108 Uplink Noise For PRB23

PM counter 3GPP name
VS.ULNoise.LeRg1PRB23
VS.ULNoise.GtRg1LeRg2PRB23
VS.ULNoise.GtRg2LeRg3PRB23
VS.ULNoise.GtRg3LeRg4PRB23
VS.ULNoise.GtRg4PRB23
VS.ULNoisePerPRBGroup.LeRg1PRBg23
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg23
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg23
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg23
VS.ULNoisePerPRBGroup.GtRg4PRBg23
Monitored class: lte.Cell

Table A-109 Uplink Noise For PRB24

PM counter 3GPP name
VS.ULNoise.LeRg1PRB24
VS.ULNoise.GtRg1LeRg2PRB24
VS.ULNoise.GtRg2LeRg3PRB24
VS.ULNoise.GtRg3LeRg4PRB24
VS.ULNoise.GtRg4PRB24
VS.ULNoisePerPRBGroup.LeRg1PRBg24
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg24
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg24
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg24
VS.ULNoisePerPRBGroup.GtRg4PRBg24
Monitored class: lte.Cell

Table A-110 Uplink Noise For PRB25

PM counter 3GPP name
VS.ULNoise.LeRg1PRB25
VS.ULNoise.GtRg1LeRg2PRB25
VS.ULNoise.GtRg2LeRg3PRB25
VS.ULNoise.GtRg3LeRg4PRB25
VS.ULNoise.GtRg4PRB25
VS.ULNoisePerPRBGroup.LeRg1PRBg25
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg25
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg25
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg25
VS.ULNoisePerPRBGroup.GtRg4PRBg25
Monitored class: lte.Cell

Table A-111 Uplink Noise For PRB26

PM counter 3GPP name
VS.ULNoise.LeRg1PRB26
VS.ULNoise.GtRg1LeRg2PRB26
VS.ULNoise.GtRg2LeRg3PRB26
VS.ULNoise.GtRg3LeRg4PRB26

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg4PRB26
Monitored class: lte.Cell

(2 of 2)

Table A-112 Uplink Noise For PRB27

PM counter 3GPP name
VS.ULNoise.LeRg1PRB27
VS.ULNoise.GtRg1LeRg2PRB27
VS.ULNoise.GtRg2LeRg3PRB27
VS.ULNoise.GtRg3LeRg4PRB27
VS.ULNoise.GtRg4PRB27
Monitored class: lte.Cell

Table A-113 Uplink Noise For PRB28

PM counter 3GPP name
VS.ULNoise.LeRg1PRB28
VS.ULNoise.GtRg1LeRg2PRB28
VS.ULNoise.GtRg2LeRg3PRB28
VS.ULNoise.GtRg3LeRg4PRB28
VS.ULNoise.GtRg4PRB28
Monitored class: lte.Cell

Table A-114 Uplink Noise For PRB29

PM counter 3GPP name
VS.ULNoise.LeRg1PRB29
VS.ULNoise.GtRg1LeRg2PRB29
VS.ULNoise.GtRg2LeRg3PRB29
VS.ULNoise.GtRg3LeRg4PRB29
VS.ULNoise.GtRg4PRB29
Monitored class: lte.Cell

Table A-115 Uplink Noise For PRB3

PM counter 3GPP name
VS.ULNoise.LeRg1PRB3
VS.ULNoise.GtRg1LeRg2PRB3
VS.ULNoise.GtRg2LeRg3PRB3
VS.ULNoise.GtRg3LeRg4PRB3
VS.ULNoise.GtRg4PRB3
VS.LeRg1PRBg3
VS.GtRg1LeRg2PRBg3
VS.GtRg2LeRg3PRBg3
VS.GtRg3LeRg4PRBg3
VS.GtRg4PRBg3
Monitored class: lte.Cell

Table A-116 Uplink Noise For PRB30

PM counter 3GPP name
VS.ULNoise.LeRg1PRB30
VS.ULNoise.GtRg1LeRg2PRB30
VS.ULNoise.GtRg2LeRg3PRB30
VS.ULNoise.GtRg3LeRg4PRB30
VS.ULNoise.GtRg4PRB30
Monitored class: lte.Cell

Table A-117 Uplink Noise For PRB31

PM counter 3GPP name
VS.ULNoise.LeRg1PRB31
VS.ULNoise.GtRg1LeRg2PRB31
VS.ULNoise.GtRg2LeRg3PRB31
VS.ULNoise.GtRg3LeRg4PRB31
VS.ULNoise.GtRg4PRB31
Monitored class: lte.Cell

Table A-118 Uplink Noise For PRB32

PM counter 3GPP name
VS.ULNoise.LeRg1PRB32
VS.ULNoise.GtRg1LeRg2PRB32
VS.ULNoise.GtRg2LeRg3PRB32
VS.ULNoise.GtRg3LeRg4PRB32
VS.ULNoise.GtRg4PRB32
Monitored class: lte.Cell

Table A-119 Uplink Noise For PRB33

PM counter 3GPP name
VS.ULNoise.LeRg1PRB33
VS.ULNoise.GtRg1LeRg2PRB33
VS.ULNoise.GtRg2LeRg3PRB33
VS.ULNoise.GtRg3LeRg4PRB33
VS.ULNoise.GtRg4PRB33
Monitored class: lte.Cell

Table A-120 Uplink Noise For PRB34

PM counter 3GPP name
VS.ULNoise.LeRg1PRB34
VS.ULNoise.GtRg1LeRg2PRB34
VS.ULNoise.GtRg2LeRg3PRB34
VS.ULNoise.GtRg3LeRg4PRB34
VS.ULNoise.GtRg4PRB34
Monitored class: lte.Cell

Table A-121 Uplink Noise For PRB35

PM counter 3GPP name
VS.ULNoise.LeRg1PRB35
VS.ULNoise.GtRg1LeRg2PRB35
VS.ULNoise.GtRg2LeRg3PRB35

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB35
VS.ULNoise.GtRg4PRB35
Monitored class: lte.Cell

(2 of 2)

Table A-122 Uplink Noise For PRB36

PM counter 3GPP name
VS.ULNoise.LeRg1PRB36
VS.ULNoise.GtRg1LeRg2PRB36
VS.ULNoise.GtRg2LeRg3PRB36
VS.ULNoise.GtRg3LeRg4PRB36
VS.ULNoise.GtRg4PRB36
Monitored class: lte.Cell

Table A-123 Uplink Noise For PRB37

PM counter 3GPP name
VS.ULNoise.LeRg1PRB37
VS.ULNoise.GtRg1LeRg2PRB37
VS.ULNoise.GtRg2LeRg3PRB37
VS.ULNoise.GtRg3LeRg4PRB37
VS.ULNoise.GtRg4PRB37
Monitored class: lte.Cell

Table A-124 Uplink Noise For PRB38

PM counter 3GPP name
VS.ULNoise.LeRg1PRB38
VS.ULNoise.GtRg1LeRg2PRB38
VS.ULNoise.GtRg2LeRg3PRB38
VS.ULNoise.GtRg3LeRg4PRB38
VS.ULNoise.GtRg4PRB38
Monitored class: lte.Cell

Table A-125 Uplink Noise For PRB39

PM counter 3GPP name
VS.ULNoise.LeRg1PRB39
VS.ULNoise.GtRg1LeRg2PRB39
VS.ULNoise.GtRg2LeRg3PRB39
VS.ULNoise.GtRg3LeRg4PRB39
VS.ULNoise.GtRg4PRB39
Monitored class: lte.Cell

Table A-126 Uplink Noise For PRB4

PM counter 3GPP name
VS.ULNoise.LeRg1PRB4
VS.ULNoise.GtRg1LeRg2PRB4
VS.ULNoise.GtRg2LeRg3PRB4
VS.ULNoise.GtRg3LeRg4PRB4
VS.ULNoise.GtRg4PRB4
VS.LeRg1PRBg4
VS.GtRg1LeRg2PRBg4
VS.GtRg2LeRg3PRBg4
VS.GtRg3LeRg4PRBg4
VS.GtRg4PRBg4
Monitored class: lte.Cell

Table A-127 Uplink Noise For PRB40

PM counter 3GPP name
VS.ULNoise.LeRg1PRB40
VS.ULNoise.GtRg1LeRg2PRB40
VS.ULNoise.GtRg2LeRg3PRB40
VS.ULNoise.GtRg3LeRg4PRB40
VS.ULNoise.GtRg4PRB40
Monitored class: lte.Cell

Table A-128 Uplink Noise For PRB41

PM counter 3GPP name
VS.ULNoise.LeRg1PRB41
VS.ULNoise.GtRg1LeRg2PRB41
VS.ULNoise.GtRg2LeRg3PRB41
VS.ULNoise.GtRg3LeRg4PRB41
VS.ULNoise.GtRg4PRB41
Monitored class: lte.Cell

Table A-129 Uplink Noise For PRB42

PM counter 3GPP name
VS.ULNoise.LeRg1PRB42
VS.ULNoise.GtRg1LeRg2PRB42
VS.ULNoise.GtRg2LeRg3PRB42
VS.ULNoise.GtRg3LeRg4PRB42
VS.ULNoise.GtRg4PRB42
Monitored class: lte.Cell

Table A-130 Uplink Noise For PRB43

PM counter 3GPP name
VS.ULNoise.LeRg1PRB43
VS.ULNoise.GtRg1LeRg2PRB43
VS.ULNoise.GtRg2LeRg3PRB43
VS.ULNoise.GtRg3LeRg4PRB43
VS.ULNoise.GtRg4PRB43
Monitored class: lte.Cell

Table A-131 Uplink Noise For PRB44

PM counter 3GPP name
VS.ULNoise.LeRg1PRB44
VS.ULNoise.GtRg1LeRg2PRB44
VS.ULNoise.GtRg2LeRg3PRB44

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB44
VS.ULNoise.GtRg4PRB44
Monitored class: lte.Cell

(2 of 2)

Table A-132 Uplink Noise For PRB45

PM counter 3GPP name
VS.ULNoise.LeRg1PRB45
VS.ULNoise.GtRg1LeRg2PRB45
VS.ULNoise.GtRg2LeRg3PRB45
VS.ULNoise.GtRg3LeRg4PRB45
VS.ULNoise.GtRg4PRB45
Monitored class: lte.Cell

Table A-133 Uplink Noise For PRB46

PM counter 3GPP name
VS.ULNoise.LeRg1PRB46
VS.ULNoise.GtRg1LeRg2PRB46
VS.ULNoise.GtRg2LeRg3PRB46
VS.ULNoise.GtRg3LeRg4PRB46
VS.ULNoise.GtRg4PRB46
Monitored class: lte.Cell

Table A-134 Uplink Noise For PRB47

PM counter 3GPP name
VS.ULNoise.LeRg1PRB47
VS.ULNoise.GtRg1LeRg2PRB47
VS.ULNoise.GtRg2LeRg3PRB47
VS.ULNoise.GtRg3LeRg4PRB47
VS.ULNoise.GtRg4PRB47
Monitored class: lte.Cell

Table A-135 Uplink Noise For PRB48

PM counter 3GPP name
VS.ULNoise.LeRg1PRB48
VS.ULNoise.GtRg1LeRg2PRB48
VS.ULNoise.GtRg2LeRg3PRB48
VS.ULNoise.GtRg3LeRg4PRB48
VS.ULNoise.GtRg4PRB48
Monitored class: lte.Cell

Table A-136 Uplink Noise For PRB49

PM counter 3GPP name
VS.ULNoise.LeRg1PRB49
VS.ULNoise.GtRg1LeRg2PRB49
VS.ULNoise.GtRg2LeRg3PRB49
VS.ULNoise.GtRg3LeRg4PRB49
VS.ULNoise.GtRg4PRB49
Monitored class: lte.Cell

Table A-137 Uplink Noise For PRB5

PM counter 3GPP name
VS.ULNoise.LeRg1PRB5
VS.ULNoise.GtRg1LeRg2PRB5
VS.ULNoise.GtRg2LeRg3PRB5
VS.ULNoise.GtRg3LeRg4PRB5
VS.ULNoise.GtRg4PRB5
VS.ULNoisePerPRBGroup.LeRg1PRBg5
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg5
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg5
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg5
VS.ULNoisePerPRBGroup.GtRg4PRBg5
Monitored class: lte.Cell

Table A-138 Uplink Noise For PRB50

PM counter 3GPP name
VS.ULNoise.LeRg1PRB50
VS.ULNoise.GtRg1LeRg2PRB50
VS.ULNoise.GtRg2LeRg3PRB50
VS.ULNoise.GtRg3LeRg4PRB50
VS.ULNoise.GtRg4PRB50
Monitored class: lte.Cell

Table A-139 Uplink Noise For PRB51

PM counter 3GPP name
VS.ULNoise.LeRg1PRB51
VS.ULNoise.GtRg1LeRg2PRB51
VS.ULNoise.GtRg2LeRg3PRB51
VS.ULNoise.GtRg3LeRg4PRB51
VS.ULNoise.GtRg4PRB51
Monitored class: lte.Cell

Table A-140 Uplink Noise For PRB52

PM counter 3GPP name
VS.ULNoise.LeRg1PRB52
VS.ULNoise.GtRg1LeRg2PRB52
VS.ULNoise.GtRg2LeRg3PRB52
VS.ULNoise.GtRg3LeRg4PRB52
VS.ULNoise.GtRg4PRB52
Monitored class: lte.Cell

Table A-141 Uplink Noise For PRB53

PM counter 3GPP name
VS.ULNoise.LeRg1PRB53
VS.ULNoise.GtRg1LeRg2PRB53
VS.ULNoise.GtRg2LeRg3PRB53

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB53
VS.ULNoise.GtRg4PRB53
Monitored class: lte.Cell

(2 of 2)

Table A-142 Uplink Noise For PRB54

PM counter 3GPP name
VS.ULNoise.LeRg1PRB54
VS.ULNoise.GtRg1LeRg2PRB54
VS.ULNoise.GtRg2LeRg3PRB54
VS.ULNoise.GtRg3LeRg4PRB54
VS.ULNoise.GtRg4PRB54
Monitored class: lte.Cell

Table A-143 Uplink Noise For PRB55

PM counter 3GPP name
VS.ULNoise.LeRg1PRB55
VS.ULNoise.GtRg1LeRg2PRB55
VS.ULNoise.GtRg2LeRg3PRB55
VS.ULNoise.GtRg3LeRg4PRB55
VS.ULNoise.GtRg4PRB55
Monitored class: lte.Cell

Table A-144 Uplink Noise For PRB56

PM counter 3GPP name
VS.ULNoise.LeRg1PRB56
VS.ULNoise.GtRg1LeRg2PRB56
VS.ULNoise.GtRg2LeRg3PRB56
VS.ULNoise.GtRg3LeRg4PRB56
VS.ULNoise.GtRg4PRB56
Monitored class: lte.Cell

Table A-145 Uplink Noise For PRB57

PM counter 3GPP name
VS.ULNoise.LeRg1PRB57
VS.ULNoise.GtRg1LeRg2PRB57
VS.ULNoise.GtRg2LeRg3PRB57
VS.ULNoise.GtRg3LeRg4PRB57
VS.ULNoise.GtRg4PRB57
Monitored class: lte.Cell

Table A-146 Uplink Noise For PRB58

PM counter 3GPP name
VS.ULNoise.LeRg1PRB58
VS.ULNoise.GtRg1LeRg2PRB58
VS.ULNoise.GtRg2LeRg3PRB58
VS.ULNoise.GtRg3LeRg4PRB58
VS.ULNoise.GtRg4PRB58
Monitored class: lte.Cell

Table A-147 Uplink Noise For PRB59

PM counter 3GPP name
VS.ULNoise.LeRg1PRB59
VS.ULNoise.GtRg1LeRg2PRB59
VS.ULNoise.GtRg2LeRg3PRB59
VS.ULNoise.GtRg3LeRg4PRB59
VS.ULNoise.GtRg4PRB59
Monitored class: lte.Cell

Table A-148 Uplink Noise For PRB6

PM counter 3GPP name
VS.ULNoise.LeRg1PRB6
VS.ULNoise.GtRg1LeRg2PRB6
VS.ULNoise.GtRg2LeRg3PRB6

(1 of 2)

A. eNodeB PM statistics counters

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB6
VS.ULNoise.GtRg4PRB6
VS.ULNoisePerPRBGroup.LeRg1PRBg6
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg6
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg6
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg6
VS.ULNoisePerPRBGroup.GtRg4PRBg6
Monitored class: lte.Cell

(2 of 2)

Table A-149 Uplink Noise For PRB60

PM counter 3GPP name
VS.ULNoise.LeRg1PRB60
VS.ULNoise.GtRg1LeRg2PRB60
VS.ULNoise.GtRg2LeRg3PRB60
VS.ULNoise.GtRg3LeRg4PRB60
VS.ULNoise.GtRg4PRB60
Monitored class: lte.Cell

Table A-150 Uplink Noise For PRB61

PM counter 3GPP name
VS.ULNoise.LeRg1PRB61
VS.ULNoise.GtRg1LeRg2PRB61
VS.ULNoise.GtRg2LeRg3PRB61
VS.ULNoise.GtRg3LeRg4PRB61
VS.ULNoise.GtRg4PRB61
Monitored class: lte.Cell

Table A-151 Uplink Noise For PRB62

PM counter 3GPP name
VS.ULNoise.LeRg1PRB62
VS.ULNoise.GtRg1LeRg2PRB62
VS.ULNoise.GtRg2LeRg3PRB62

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB62
VS.ULNoise.GtRg4PRB62
Monitored class: lte.Cell

(2 of 2)

Table A-152 Uplink Noise For PRB63

PM counter 3GPP name
VS.ULNoise.LeRg1PRB63
VS.ULNoise.GtRg1LeRg2PRB63
VS.ULNoise.GtRg2LeRg3PRB63
VS.ULNoise.GtRg3LeRg4PRB63
VS.ULNoise.GtRg4PRB63
Monitored class: lte.Cell

Table A-153 Uplink Noise For PRB64

PM counter 3GPP name
VS.ULNoise.LeRg1PRB64
VS.ULNoise.GtRg1LeRg2PRB64
VS.ULNoise.GtRg2LeRg3PRB64
VS.ULNoise.GtRg3LeRg4PRB64
VS.ULNoise.GtRg4PRB64
Monitored class: lte.Cell

Table A-154 Uplink Noise For PRB65

PM counter 3GPP name
VS.ULNoise.LeRg1PRB65
VS.ULNoise.GtRg1LeRg2PRB65
VS.ULNoise.GtRg2LeRg3PRB65
VS.ULNoise.GtRg3LeRg4PRB65
VS.ULNoise.GtRg4PRB65
Monitored class: lte.Cell

Table A-155 Uplink Noise For PRB66

PM counter 3GPP name
VS.ULNoise.LeRg1PRB66
VS.ULNoise.GtRg1LeRg2PRB66
VS.ULNoise.GtRg2LeRg3PRB66
VS.ULNoise.GtRg3LeRg4PRB66
VS.ULNoise.GtRg4PRB66
Monitored class: lte.Cell

Table A-156 Uplink Noise For PRB67

PM counter 3GPP name
VS.ULNoise.LeRg1PRB67
VS.ULNoise.GtRg1LeRg2PRB67
VS.ULNoise.GtRg2LeRg3PRB67
VS.ULNoise.GtRg3LeRg4PRB67
VS.ULNoise.GtRg4PRB67
Monitored class: lte.Cell

Table A-157 Uplink Noise For PRB68

PM counter 3GPP name
VS.ULNoise.LeRg1PRB68
VS.ULNoise.GtRg1LeRg2PRB68
VS.ULNoise.GtRg2LeRg3PRB68
VS.ULNoise.GtRg3LeRg4PRB68
VS.ULNoise.GtRg4PRB68
Monitored class: lte.Cell

Table A-158 Uplink Noise For PRB69

PM counter 3GPP name
VS.ULNoise.LeRg1PRB69
VS.ULNoise.GtRg1LeRg2PRB69
VS.ULNoise.GtRg2LeRg3PRB69

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB69
VS.ULNoise.GtRg4PRB69
Monitored class: lte.Cell

(2 of 2)

Table A-159 Uplink Noise For PRB7

PM counter 3GPP name
VS.ULNoise.LeRg1PRB7
VS.ULNoise.GtRg1LeRg2PRB7
VS.ULNoise.GtRg2LeRg3PRB7
VS.ULNoise.GtRg3LeRg4PRB7
VS.ULNoise.GtRg4PRB7
VS.ULNoisePerPRBGroup.LeRg1PRBg7
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg7
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg7
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg7
VS.ULNoisePerPRBGroup.GtRg4PRBg7
Monitored class: lte.Cell

Table A-160 Uplink Noise For PRB70

PM counter 3GPP name
VS.ULNoise.LeRg1PRB70
VS.ULNoise.GtRg1LeRg2PRB70
VS.ULNoise.GtRg2LeRg3PRB70
VS.ULNoise.GtRg3LeRg4PRB70
VS.ULNoise.GtRg4PRB70
Monitored class: lte.Cell

Table A-161 Uplink Noise For PRB71

PM counter 3GPP name
VS.ULNoise.LeRg1PRB71
VS.ULNoise.GtRg1LeRg2PRB71
VS.ULNoise.GtRg2LeRg3PRB71

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB71
VS.ULNoise.GtRg4PRB71
Monitored class: lte.Cell

(2 of 2)

Table A-162 Uplink Noise For PRB72

PM counter 3GPP name
VS.ULNoise.LeRg1PRB72
VS.ULNoise.GtRg1LeRg2PRB72
VS.ULNoise.GtRg2LeRg3PRB72
VS.ULNoise.GtRg3LeRg4PRB72
VS.ULNoise.GtRg4PRB72
Monitored class: lte.Cell

Table A-163 Uplink Noise For PRB73

PM counter 3GPP name
VS.ULNoise.LeRg1PRB73
VS.ULNoise.GtRg1LeRg2PRB73
VS.ULNoise.GtRg2LeRg3PRB73
VS.ULNoise.GtRg3LeRg4PRB73
VS.ULNoise.GtRg4PRB73
Monitored class: lte.Cell

Table A-164 Uplink Noise For PRB74

PM counter 3GPP name
VS.ULNoise.LeRg1PRB74
VS.ULNoise.GtRg1LeRg2PRB74
VS.ULNoise.GtRg2LeRg3PRB74
VS.ULNoise.GtRg3LeRg4PRB74
VS.ULNoise.GtRg4PRB74
Monitored class: lte.Cell

Table A-165 Uplink Noise For PRB75

PM counter 3GPP name
VS.ULNoise.LeRg1PRB75
VS.ULNoise.GtRg1LeRg2PRB75
VS.ULNoise.GtRg2LeRg3PRB75
VS.ULNoise.GtRg3LeRg4PRB75
VS.ULNoise.GtRg4PRB75
Monitored class: lte.Cell

Table A-166 Uplink Noise For PRB76

PM counter 3GPP name
VS.ULNoise.LeRg1PRB76
VS.ULNoise.GtRg1LeRg2PRB76
VS.ULNoise.GtRg2LeRg3PRB76
VS.ULNoise.GtRg3LeRg4PRB76
VS.ULNoise.GtRg4PRB76
Monitored class: lte.Cell

Table A-167 Uplink Noise For PRB77

PM counter 3GPP name
VS.ULNoise.LeRg1PRB77
VS.ULNoise.GtRg1LeRg2PRB77
VS.ULNoise.GtRg2LeRg3PRB77
VS.ULNoise.GtRg3LeRg4PRB77
VS.ULNoise.GtRg4PRB77
Monitored class: lte.Cell

Table A-168 Uplink Noise For PRB78

PM counter 3GPP name
VS.ULNoise.LeRg1PRB78
VS.ULNoise.GtRg1LeRg2PRB78
VS.ULNoise.GtRg2LeRg3PRB78

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB78
VS.ULNoise.GtRg4PRB78
Monitored class: lte.Cell

(2 of 2)

Table A-169 Uplink Noise For PRB79

PM counter 3GPP name
VS.ULNoise.LeRg1PRB79
VS.ULNoise.GtRg1LeRg2PRB79
VS.ULNoise.GtRg2LeRg3PRB79
VS.ULNoise.GtRg3LeRg4PRB79
VS.ULNoise.GtRg4PRB79
Monitored class: lte.Cell

Table A-170 Uplink Noise For PRB8

PM counter 3GPP name
VS.ULNoise.LeRg1PRB8
VS.ULNoise.GtRg1LeRg2PRB8
VS.ULNoise.GtRg2LeRg3PRB8
VS.ULNoise.GtRg3LeRg4PRB8
VS.ULNoise.GtRg4PRB8
VS.ULNoisePerPRBGroup.LeRg1PRBg8
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg8
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg8
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg8
VS.ULNoisePerPRBGroup.GtRg4PRBg8
Monitored class: lte.Cell

Table A-171 Uplink Noise For PRB80

PM counter 3GPP name
VS.ULNoise.LeRg1PRB80
VS.ULNoise.GtRg1LeRg2PRB80
VS.ULNoise.GtRg2LeRg3PRB80

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB80
VS.ULNoise.GtRg4PRB80
Monitored class: lte.Cell

(2 of 2)

Table A-172 Uplink Noise For PRB81

PM counter 3GPP name
VS.ULNoise.LeRg1PRB81
VS.ULNoise.GtRg1LeRg2PRB81
VS.ULNoise.GtRg2LeRg3PRB81
VS.ULNoise.GtRg3LeRg4PRB81
VS.ULNoise.GtRg4PRB81
Monitored class: lte.Cell

Table A-173 Uplink Noise For PRB82

PM counter 3GPP name
VS.ULNoise.LeRg1PRB82
VS.ULNoise.GtRg1LeRg2PRB82
VS.ULNoise.GtRg2LeRg3PRB82
VS.ULNoise.GtRg3LeRg4PRB82
VS.ULNoise.GtRg4PRB82
Monitored class: lte.Cell

Table A-174 Uplink Noise For PRB83

PM counter 3GPP name
VS.ULNoise.LeRg1PRB83
VS.ULNoise.GtRg1LeRg2PRB83
VS.ULNoise.GtRg2LeRg3PRB83
VS.ULNoise.GtRg3LeRg4PRB83
VS.ULNoise.GtRg4PRB83
Monitored class: lte.Cell

Table A-175 Uplink Noise For PRB84

PM counter 3GPP name
VS.ULNoise.LeRg1PRB84
VS.ULNoise.GtRg1LeRg2PRB84
VS.ULNoise.GtRg2LeRg3PRB84
VS.ULNoise.GtRg3LeRg4PRB84
VS.ULNoise.GtRg4PRB84
Monitored class: lte.Cell

Table A-176 Uplink Noise For PRB85

PM counter 3GPP name
VS.ULNoise.LeRg1PRB85
VS.ULNoise.GtRg1LeRg2PRB85
VS.ULNoise.GtRg2LeRg3PRB85
VS.ULNoise.GtRg3LeRg4PRB85
VS.ULNoise.GtRg4PRB85
Monitored class: lte.Cell

Table A-177 Uplink Noise For PRB86

PM counter 3GPP name
VS.ULNoise.LeRg1PRB86
VS.ULNoise.GtRg1LeRg2PRB86
VS.ULNoise.GtRg2LeRg3PRB86
VS.ULNoise.GtRg3LeRg4PRB86
VS.ULNoise.GtRg4PRB86
Monitored class: lte.Cell

Table A-178 Uplink Noise For PRB87

PM counter 3GPP name
VS.ULNoise.LeRg1PRB87
VS.ULNoise.GtRg1LeRg2PRB87
VS.ULNoise.GtRg2LeRg3PRB87

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB87
VS.ULNoise.GtRg4PRB87
Monitored class: lte.Cell

(2 of 2)

Table A-179 Uplink Noise For PRB88

PM counter 3GPP name
VS.ULNoise.LeRg1PRB88
VS.ULNoise.GtRg1LeRg2PRB88
VS.ULNoise.GtRg2LeRg3PRB88
VS.ULNoise.GtRg3LeRg4PRB88
VS.ULNoise.GtRg4PRB88
Monitored class: lte.Cell

Table A-180 Uplink Noise For PRB89

PM counter 3GPP name
VS.ULNoise.LeRg1PRB89
VS.ULNoise.GtRg1LeRg2PRB89
VS.ULNoise.GtRg2LeRg3PRB89
VS.ULNoise.GtRg3LeRg4PRB89
VS.ULNoise.GtRg4PRB89
Monitored class: lte.Cell

Table A-181 Uplink Noise For PRB9

PM counter 3GPP name
VS.ULNoise.LeRg1PRB9
VS.ULNoise.GtRg1LeRg2PRB9
VS.ULNoise.GtRg2LeRg3PRB9
VS.ULNoise.GtRg3LeRg4PRB9
VS.ULNoise.GtRg4PRB9
VS.ULNoisePerPRBGroup.LeRg1PRBg9
VS.ULNoisePerPRBGroup.GtRg1LeRg2PRBg9
VS.ULNoisePerPRBGroup.GtRg2LeRg3PRBg9

(1 of 2)

PM counter 3GPP name
VS.ULNoisePerPRBGroup.GtRg3LeRg4PRBg9
VS.ULNoisePerPRBGroup.GtRg4PRBg9
Monitored class: lte.Cell

(2 of 2)

Table A-182 Uplink Noise For PRB90

PM counter 3GPP name
VS.ULNoise.LeRg1PRB90
VS.ULNoise.GtRg1LeRg2PRB90
VS.ULNoise.GtRg2LeRg3PRB90
VS.ULNoise.GtRg3LeRg4PRB90
VS.ULNoise.GtRg4PRB90
Monitored class: lte.Cell

Table A-183 Uplink Noise For PRB91

PM counter 3GPP name
VS.ULNoise.LeRg1PRB91
VS.ULNoise.GtRg1LeRg2PRB91
VS.ULNoise.GtRg2LeRg3PRB91
VS.ULNoise.GtRg3LeRg4PRB91
VS.ULNoise.GtRg4PRB91
Monitored class: lte.Cell

Table A-184 Uplink Noise For PRB92

PM counter 3GPP name
VS.ULNoise.LeRg1PRB92
VS.ULNoise.GtRg1LeRg2PRB92
VS.ULNoise.GtRg2LeRg3PRB92
VS.ULNoise.GtRg3LeRg4PRB92
VS.ULNoise.GtRg4PRB92
Monitored class: lte.Cell

Table A-185 Uplink Noise For PRB93

PM counter 3GPP name
VS.ULNoise.LeRg1PRB93
VS.ULNoise.GtRg1LeRg2PRB93
VS.ULNoise.GtRg2LeRg3PRB93
VS.ULNoise.GtRg3LeRg4PRB93
VS.ULNoise.GtRg4PRB93
Monitored class: lte.Cell

Table A-186 Uplink Noise For PRB94

PM counter 3GPP name
VS.ULNoise.LeRg1PRB94
VS.ULNoise.GtRg1LeRg2PRB94
VS.ULNoise.GtRg2LeRg3PRB94
VS.ULNoise.GtRg3LeRg4PRB94
VS.ULNoise.GtRg4PRB94
Monitored class: lte.Cell

Table A-187 Uplink Noise For PRB95

PM counter 3GPP name
VS.ULNoise.LeRg1PRB95
VS.ULNoise.GtRg1LeRg2PRB95
VS.ULNoise.GtRg2LeRg3PRB95
VS.ULNoise.GtRg3LeRg4PRB95
VS.ULNoise.GtRg4PRB95
Monitored class: lte.Cell

Table A-188 Uplink Noise For PRB96

PM counter 3GPP name
VS.ULNoise.LeRg1PRB96
VS.ULNoise.GtRg1LeRg2PRB96
VS.ULNoise.GtRg2LeRg3PRB96

(1 of 2)

PM counter 3GPP name
VS.ULNoise.GtRg3LeRg4PRB96
VS.ULNoise.GtRg4PRB96
Monitored class: lte.Cell

(2 of 2)

Table A-189 Uplink Noise For PRB97

PM counter 3GPP name
VS.ULNoise.LeRg1PRB97
VS.ULNoise.GtRg1LeRg2PRB97
VS.ULNoise.GtRg2LeRg3PRB97
VS.ULNoise.GtRg3LeRg4PRB97
VS.ULNoise.GtRg4PRB97
Monitored class: lte.Cell

Table A-190 Uplink Noise For PRB98

PM counter 3GPP name
VS.ULNoise.LeRg1PRB98
VS.ULNoise.GtRg1LeRg2PRB98
VS.ULNoise.GtRg2LeRg3PRB98
VS.ULNoise.GtRg3LeRg4PRB98
VS.ULNoise.GtRg4PRB98
Monitored class: lte.Cell

Table A-191 Uplink Noise For PRB99

PM counter 3GPP name
VS.ULNoise.LeRg1PRB99
VS.ULNoise.GtRg1LeRg2PRB99
VS.ULNoise.GtRg2LeRg3PRB99
VS.ULNoise.GtRg3LeRg4PRB99
VS.ULNoise.GtRg4PRB99
Monitored class: lte.Cell

Table A-192 Uplink Paired Grants per TTI Stats

PM counter 3GPP name
VS.ULPairedGrant.0Grant
VS.ULPairedGrant.1Grants
VS.ULPairedGrant.2Grants
Monitored class: lte.Cell

Table A-193 VoIP downlink FER Stats

PM counter 3GPP name
VS.VolPDLFER.LeRange1
VS.VolPDLFER.GTRange1LeRange2
VS.VolPDLFER.GTRange2LeRange3
VS.VolPDLFER.GTRange3LeRange4
VS.VolPDLFER.GTRange4
VS.VolPDLFER.LeRange1
VS.VolPDLFER.GTRange1LeRange2
VS.VolPDLFER.GTRange2LeRange3
VS.VolPDLFER.GTRange3LeRange4
VS.VolPDLFER.GTRange4
Monitored class: lte.Cell

Table A-194 Wideband CQI Reported in Tx Diversity Stats

PM counter 3GPP name
VS.Layer0TxDivWBCqiReported.Cqi0
VS.Layer0TxDivWBCqiReported.Cqi1
VS.Layer0TxDivWBCqiReported.Cqi2
VS.Layer0TxDivWBCqiReported.Cqi3
VS.Layer0TxDivWBCqiReported.Cqi4
VS.Layer0TxDivWBCqiReported.Cqi5
VS.Layer0TxDivWBCqiReported.Cqi6
VS.Layer0TxDivWBCqiReported.Cqi7
VS.Layer0TxDivWBCqiReported.Cqi8
VS.Layer0TxDivWBCqiReported.Cqi9
VS.Layer0TxDivWBCqiReported.Cqi10

(1 of 2)

PM counter 3GPP name
VS.Layer0TxDivWBCqiReported.Cqi11
VS.Layer0TxDivWBCqiReported.Cqi12
VS.Layer0TxDivWBCqiReported.Cqi13
VS.Layer0TxDivWBCqiReported.Cqi14
VS.Layer0TxDivWBCqiReported.Cqi15
Monitored class: lte.Cell

(2 of 2)

Table A-195 X2 SCTP Traffic Stats

PM counter 3GPP name
VS.X2SctpInOctets
VS.X2SctpInPackets
VS.X2SctpOutOctets
VS.X2SctpOutPackets
Monitored class: lte.X2Access

A.2 eNodeB interface statistics

This section describes the interface statistics counters for all supported versions of the eNodeB. Table A-196 lists the statistics classes.

Table A-196 Statistics packages and counter tables

Package name	See
equipment	Table A-197

Table A-197 equipment statistics

5620 SAM counter name	Type	MIB counter name	Description
InterfaceStats MIB table name: IF-MIB.ifTable Monitored classes: equipment.PhysicalPort; equipment.ManagementPort; lag.Interface; bundle.Interface; sonetequipment.Sts1Channel; sonetequipment.Sts3Channel; sonetequipment.Sts12Channel; sonetequipment.Sts48Channel; sonetequipment.Sts192Channel; tdmequipment.DS3E3Channel; tdmequipment.DS1E1Channel; tdmequipment.DS0ChannelGroup; ccag.CcagPathCcNetSap; ccag.CcagPathCcSapNet; ccag.CcagPathCcSapSap; sonetequipment.Tu3Channel; sonetequipment.TributaryChannel			

(1 of 3)

5620 SAM counter name	Type	MIB counter name	Description
outboundBadPackets	long	ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
outboundPacketsDiscarded	long	ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedBadPackets	long	ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedOctets	long	ifInOctets	The total number of octets received on the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedPacketsDiscarded	long	ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

(2 of 3)

A. eNodeB PM statistics counters

5620 SAM counter name	Type	MIB counter name	Description
receivedUnicastPackets	long	ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedUnknownProtocolPackets	long	ifInUnknownProtos	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
transmittedOctets	long	ifOutOctets	The total number of octets transmitted out of the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
transmittedUnicastPackets	long	ifOutUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

(3 of 3)

B. RAN licenses

B.1 RAN license parameter mapping *B-2*

B.2 LA2.0 *B-2*

B.3 TLA2.1 *B-3*

B.4 LA3.0 *B-3*

B.5 TLA3.0 *B-4*

B.6 LA 4.0 *B-5*

B.7 TLA4.0 *B-6*

B.1 RAN license parameter mapping

This appendix describes the mapping between eNodeB parameter objects and RAN license entitlements for all versions of the eNodeB that the 5620 SAM supports. The following mapping information is described:

- eNodeB parameter name
- parent object hierarchy (eNodeB MIM)
- license entitlement name

The mapping information provided by this appendix is intended to assist in online and offline configuration of license-impacting parameters. The object hierarchy in this appendix uses the object naming convention of the eNodeB MIM. Table B-1 describes the object name mapping for the following domains:

- eNodeB MIM—The object naming used in the eNodeB database, parameter documentation, the 9952 WPS, and WO files.
- 5620 SAM schema—The object naming used in the 5620 SAM schema for online configuration over OSS interface.
- 5620 SAM GUI—The object naming used in the 5620 SAM GUI for component trees in object Properties forms.



Note — The following table lists mapping for objects that differ on name and spelling. The table does not list mapping for objects that differ only on capitalization and/or spacing, such as `LteCellFDD` (eNodeB MIM) and `LTE Cell FDD` (5620 SAM GUI).

Table B-1 Object mapping between eNodeB MIM and 5620 SAM schema

eNodeB MIM	5620 SAM schema	5620 SAM GUI
Enb	ENBNEspecifics	eNodeB NE Instance
LteCell	Cell	Cell
RadioCacEnb	RadioCacEnb	Radio CAC eNodeB
SubscAndEquipmentTraces	SubscAndEquipmentTraces	Subscriber And Equipment Traces

B.2 LA2.0

Table B-2 lists the RAN license mapping for LA2.0.

Table B-2 LA2.0 license mapping

Parameter name	Parent object	License names
dlBandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthFDD	<ul style="list-style-type: none"> isDLBandwidth1MhzAllowed isDLBandwidth3MhzAllowed isDLBandwidth5MhzAllowed isDLBandwidth10MhzAllowed isDLBandwidth20MhzAllowed
ulBandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthFDD	<ul style="list-style-type: none"> isULBandwidth1MhzAllowed isULBandwidth3MhzAllowed isULBandwidth5MhzAllowed isULBandwidth10MhzAllowed isULBandwidth20MhzAllowed
maxNumberOfCallPerEnodeB	ENBEquipment/Enb/RrmServices/RadioCacEnb	maxNbOfCallCapacityLicensing
cellDLTotalPower	ENBEquipment/Enb/LteCell	transmissionPowerCapacityLicensing
numberOfDLAntennas	ENBEquipment/Enb/LteCell/LteCellFDD	transmissionPowerCapacityLicensing

B.3 TLA2.1

RAN licensing is not supported for TLA2.1.

B.4 LA3.0

Table B-3 lists the RAN license mapping for LA3.0.

Table B-3 LA3.0 license mapping

Parameter name	Parent object	License names
dlBandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthFDD	<ul style="list-style-type: none"> isDLBandwidth1MhzAllowed isDLBandwidth3MhzAllowed isDLBandwidth5MhzAllowed isDLBandwidth10MhzAllowed isDLBandwidth15MhzAllowed isDLBandwidth20MhzAllowed
ulBandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthFDD	<ul style="list-style-type: none"> isULBandwidth1MhzAllowed isULBandwidth3MhzAllowed isULBandwidth5MhzAllowed isULBandwidth10MhzAllowed isULBandwidth15MhzAllowed isULBandwidth20MhzAllowed
anrEnable	ENBEquipment/Enb/ActivationService	anrEnable
isPCMDEnabled	ENBEquipment/Enb/SubscAndEquipmentTraces	isPCMDEnabled
isMobilityToHrpdAllowed	ENBEquipment/Enb/ActivationService	isMobilityToHrpdAllowed

(1 of 2)

Parameter name	Parent object	License names
isCsFallbackToGeranAllowed	ENBEquipment/Enb/ActivationService	isCsFallbackToGeranAllowed
isCsFallbackToUtraFddAllowed	ENBEquipment/Enb/ActivationService	isCsFallbackToUtraFddAllowed
isMobilityToUtranAllowed	ENBEquipment/Enb/ActivationService	isMobilityToUtranAllowed
isMobilityToGeranAllowed	ENBEquipment/Enb/ActivationService	isMobilityToGeranAllowed
isIPsecEnabled	ENBEquipment/Enb/ActivationService	isIPsecEnabled
isInterFreqEutraSameFrameStructureMobilityAllowed	ENBEquipment/Enb/ActivationService	isInterFreqEutraSameFrameStructureMobilityAllowed
isServiceBasedTrafficSegmentationAllowed	ENBEquipment/Enb/ActivationService	isServiceBasedTrafficSegmentationAllowed
isEnbSelfConfigAllowed	ENBEquipment/Enb/ActivationService	LTEisENbSelfConfigAllowed
isSonPciAllocationEnabled	ENBEquipment/Enb/ActivationService	isSonPciAllocationEnabled
isCsfbEnhancedRedirectionEnabled	ENBEquipment/Enb/ActivationService	isCsfbEnhancedRedirectionEnabled
maxNumberOfCallPerEnodeB	ENBEquipment/Enb/RrmServices/RadioCacEnb	maxNbOfCallCapacityLicensing
cellDLTotalPower	ENBEquipment/Enb/LteCell	transmissionPowerCapacityLicensing
numberOfDLAntennas	ENBEquipment/Enb/LteCell/LteCellFDD	transmissionPowerCapacityLicensing

(2 of 2)

B.5 TLA3.0

Table B-4 lists the RAN license mapping for TLA3.0.

Table B-4 TLA3.0 license mapping

Parameter name	Parent object	License names
bandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthTDD	<ul style="list-style-type: none"> isDLBandwidth10MhzAllowed isDLBandwidth20MhzAllowed
anrEnable	ENBEquipment/Enb/ActivationService	LTEanrEnable
isPCMDEnabled	ENBEquipment/Enb/SubscAndEquipmentTraces	LTEisPCMDEnabled
isIPsecEnabled	ENBEquipment/Enb/ActivationService	LTEisIPsecEnabled
isInterFreqEutraSameFrameStructureMobilityAllowed	ENBEquipment/Enb/ActivationService	LTEisInterFreqEutraSameFrameStructureMobilityAllowed
isServiceBasedTrafficSegmentationAllowed	ENBEquipment/Enb/ActivationService	LTEisServiceBasedTrafficSegmentationAllowed
isEnbSelfConfigAllowed	ENBEquipment/Enb/ActivationService	LTEisEnbSelfConfigAllowed
isSonPciAllocationEnabled	ENBEquipment/Enb/ActivationService	LTEisSonPciAllocationEnabled
isMbmsBroadcastModeAllowed	ENBEquipment/Enb/ActivationService	LTEisMbmsBroadcastModeAllowed
maxNumberOfCallPerEnodeB	ENBEquipment/Enb/RrmServices/RadioCacEnb	maxNbOfCallCapacityLicensing

(1 of 2)

Parameter name	Parent object	License names
cellDLTotalPower	ENBEquipment/Enb/LteCell	transmissionPowerCapacityLicensing
numberOfDLAntennas	ENBEquipment/Enb/LteCell/LteCellTDD	transmissionPowerCapacityLicensing

(2 of 2)

B.6 LA 4.0

Table B-5 lists the RAN license mapping for LA 4.0.

Table B-5 LA4.0 license mapping

Parameter name	Parent object	License names
dLBandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthFDD	<ul style="list-style-type: none"> isDLBandwidth5MhzAllowed isDLBandwidth10MhzAllowed isDLBandwidth15MhzAllowed isDLBandwidth20MhzAllowed
uLBandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthFDD	<ul style="list-style-type: none"> isULBandwidth5MhzAllowed isULBandwidth10MhzAllowed isULBandwidth15MhzAllowed isULBandwidth20MhzAllowed
isPCMDEnabled	ENBEquipment/Enb/SubscAndEquipmentTraces	LTEisPCMDEnabled
isMobilityToHrpdAllowed	ENBEquipment/Enb/ActivationService	LTEisMobilityToHrpdAllowed
isCsFallbackToGeranAllowed	ENBEquipment/Enb/ActivationService	LTEisCsFallbackToGeranAllowed
isCsFallbackToUtraAllowed	ENBEquipment/Enb/ActivationService	LTEisCsFallbackToUtraFddAllowed
isMobilityToUtranAllowed	ENBEquipment/Enb/ActivationService	LTEisMobilityToUtranAllowed
isMobilityToGeranAllowed	ENBEquipment/Enb/ActivationService	LTEisMobilityToGeranAllowed
isIPsecEnabled	ENBEquipment/Enb/ActivationService	LTEisIPsecEnable
isInterFreqEutraSameFrameStructureMobilityAllowed	ENBEquipment/Enb/ActivationService	LTEisInterFreqEutraSameFrameStructureMobilityAllowed
isServiceBasedTrafficSegmentationAllowed	ENBEquipment/Enb/ActivationService	LTEisServiceBasedTrafficSegmentationAllowed
isEnbSelfConfigAllowed	ENBEquipment/Enb/ActivationService	LTEisENBselfConfigAllowed
isSonPciAllocationEnabled	ENBEquipment/Enb/ActivationService	LTEisSonPciAllocationEnabled
lteIntraFrequencyAnrEnabled	ENBEquipment/Enb/ActivationService	LTEAnrEnable
isFiberDelayAllowed	ENBEquipment/Enb/LteCell/CellActivationService	LTEisFiberDelayAllowed
isCsfbEnhancedRedirectionAndPsHoAllowed	ENBEquipment/Enb/ActivationService	LTEisCsfbEnhancedRedirectionAndPsHoAllowed
utraAnrEnabled	ENBEquipment/Enb/ActivationService	LTEutraAnrEnabled
isCsfbTo1xRttForDRxUEallowed	ENBEquipment/Enb/ActivationService	LTEisCsfbTo1xRttForDRxUEallowed
isCmasEnabled	ENBEquipment/Enb/ActivationService	LTEisCmasEnabled

(1 of 2)

B. RAN licenses

Parameter name	Parent object	License names
isOffLoadUponReactiveLoadControlAllowed	ENBEquipment/Enb/ActivationService	LTEisOffLoadUponReactiveLoadControlAllowed
maxNbOfDataBearersPerUe	ENBEquipment/Enb/RrmServices/RadioCacEnb	<ul style="list-style-type: none">• LTEis4Bearers• LTEis5Bearers• LTEis6Bearers• LTEis7Bearers• LTEis8Bearers
lteInterFrequencyAnrForUETestEnabled	ENBEquipment/Enb/ActivationService	LTElteInterFrequencyAnrForUETestEnabled
isGeoLocPhaseSyncAllowed	ENBEquipment/Enb/ActivationService	LTEisGeoLocPhaseSyncAllowed
isEcidSupportAllowed	ENBEquipment/Enb/ActivationService	LTEisEcidSupportAllowed
isSpsConfigAllowed	ENBEquipment/Enb/ActivationService	LTEisSpsConfigAllowed
isRohcAllowed	ENBEquipment/Enb/ActivationService	LTEisRohcAllowed
isDasDelayEnabled	ENBEquipment/Enb/LteCell/CellActivationService	LTEisDasDelayEnabled
isAisgAllowed	ENBEquipment/Enb/ActivationService	LTEisAisgAllowed
maxNbPlmnForMocnLicense	ENBEquipment/Enb/LicensingMngtSystem	LTEmax2PlmnForMocnLicense
transmissionMode	ENBEquipment/Enb/LteCell/LteCellFDD	LTEis1AntennaTransmitMode
maxNumberOfCallPerEnodeB	ENBEquipment/Enb/RrmServices/RadioCacEnb	maxNbOfCallCapacityLicensing
cellDLTotalPower	ENBEquipment/Enb/LteCell	transmissionPowerCapacityLicensing
numberOfDLAntennas	ENBEquipment/Enb/LteCell/LteCellFDD	transmissionPowerCapacityLicensing
numberOfULAntennas	ENBEquipment/Enb/LteCell/LteCellFDD	LTEis4RxDiversityAllowed

(2 of 2)

B.7 TLA4.0

Table B-6 lists the RAN license mapping for TLA4.0.

Table B-6 TLA4.0 license mapping

Parameter name	Parent object	License names
bandwidth	ENBEquipment/Enb/LteCell/FrequencyAndBandwidthTDD	<ul style="list-style-type: none">• isDLBandwidth10MhzAllowed• isDLBandwidth20MhzAllowed
anrEnable	ENBEquipment/Enb/ActivationService	LTEAnrEnable
isPCMDEnabled	ENBEquipment/Enb/SubscAndEquipmentTraces	LTEisPCMDEnabled
isIPsecEnabled	ENBEquipment/Enb/ActivationService	LTEisIPsecEnabled
isInterFreqEutraSameFrameStructureMobilityAllowed	ENBEquipment/Enb/ActivationService	LTEisInterFreqEutraSameFrameStructureMobilityAllowed
isServiceBasedTrafficSegmentationAllowed	ENBEquipment/Enb/ActivationService	LTEisServiceBasedTrafficSegmentationAllowed
isEnbSelfConfigAllowed	ENBEquipment/Enb/ActivationService	LTEisEnbSelfConfigAllowed

(1 of 2)

Parameter name	Parent object	License names
isSonPciAllocationEnabled	ENBEquipment/Enb/ActivationService	LTEisSonPciAllocationEnabled
isMbmsBroadcastModeAllowed	ENBEquipment/Enb/ActivationService	LTEisMbmsBroadcastModeAllowed
maxNumberOfCallPerEnodeB	ENBEquipment/Enb/RrmServices/RadioCacEnb	maxNbOfCallCapacityLicensing
cellDLTotalPower	ENBEquipment/Enb/LteCell	transmissionPowerCapacityLicensing
numberOfDLAntennas	ENBEquipment/Enb/LteCell/LteCellTDD	transmissionPowerCapacityLicensing
numberOfULAntennas	ENBEquipment/Enb/LteCell/LteCellTDD	LTEis4RxDiversityAllowed
transmissionMode	ENBEquipment/Enb/LteCell/LteCellTDD	LTEisBeamformingAllowed
l1ReceiverMethod	ENBEquipment/Enb/LteCell/CellL1ULConf/CellL1ULConfTDD	LTEisIRCReceiverAllowed

(2 of 2)

Customer documentation and product support



Customer documentation

<http://www.alcatel-lucent.com/myaccess>

Product manuals and documentation updates are available at [alcatel-lucent.com](http://www.alcatel-lucent.com). If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.



Technical Support

<http://support.alcatel-lucent.com>



Documentation feedback

documentation.feedback@alcatel-lucent.com

