



Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 9.0 R7
PLANNING GUIDE

3HE 06557 AAAJ 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
 1 — Introduction	 1-1
1.1 Overview	1-2
1.2 Purpose	1-2
1.3 Intended audience	1-2
1.4 Document changes	1-2
 2 — Product deployment overview	 2-1
2.1 5620 SAM architecture	2-2
2.2 5620 SAM Auxiliary Statistics Collector	2-5
2.3 5620 SAM Auxiliary Call Trace Collector.....	2-5
2.4 5620 SAM Client Delegate.....	2-6
2.5 5620 SAM key technology overview	2-6
Java Virtual Machine.....	2-6
Oracle database	2-7
2.6 Redundancy architecture	2-7
Redundancy and 5620 SAM Auxiliary workstations	2-9

2.7	Redundancy deployment considerations for 5620 SAM.....	2-11
	Redundancy with collocated 5620 SAM Server/Database:	2-11
	Redundancy with distributed 5620 SAM Server and 5620 SAM Database:	2-11
	Redundancy with distributed 5620 SAM Server and 5620 SAM Database and 5620 SAM Auxiliary workstations:.....	2-12
3	— Operating systems specifications	3-1
3.1	Solaris (Oracle and HP platforms)	3-2
3.2	Microsoft Windows	3-2
3.3	Operating system summary	3-3
3.4	5620 SAM Client or Delegate software requirements.....	3-3
4	— Hardware platform requirements	4-1
4.1	Hardware platform requirements overview.....	4-2
4.2	Minimum hardware platform requirements	4-2
	Minimum hardware platform requirements for Solaris.....	4-3
	Oracle or HP x86 hardware configuration:	4-3
	Oracle SPARC hardware configuration:	4-4
	Scaling limits for collocated platforms	4-5
	Minimum hardware platform requirements for 5620 SAM Auxiliary workstations.....	4-6
	Hardware platform requirements for 5620 SAM Client Delegate workstations.....	4-6
4.3	5620 SAM-O 3GPP Interface	4-7
4.4	5620 SAM GUI Client hardware platform requirements	4-8
4.5	Determining hardware platform requirements for larger networks.....	4-8
4.6	Solaris workstation disk configuration	4-9
	Using RAID technologies.....	4-10
	Using SAN storage	4-10
5	— NE maintenance	5-1
5.1	Mechanism to maintain current state of network elements.....	5-2
5.2	IP connectivity (ping) verification	5-2
5.3	SNMP connectivity verification.....	5-2
5.4	SNMP traps	5-3
5.5	SNMP trap sequence verification	5-3
5.6	Scheduled SNMP MIB polling	5-3
5.7	Network outages	5-3
6	— Network requirements	6-1
6.1	Network requirements	6-2
6.2	Connectivity to the network elements	6-2
6.3	Bandwidth requirements for collocated 5620 SAM installations	6-2
6.4	Bandwidth requirements for distributed 5620 SAM installations	6-3
	5620 SAM Auxiliary Call Trace Collectors.....	6-6
6.5	Bandwidth requirements for 5620 SAM GUI Clients.....	6-6

6.6	Bandwidth requirements for displaying 5620 SAM GUI Clients on X displays	6-7
6.7	Bandwidth requirements for 5620 SAM-O OSS Clients	6-7
6.8	Bandwidth requirements for the 5620 SAM Auxiliary Statistics Collector workstation.....	6-8
6.9	Bandwidth requirements for the 5620 SAM Auxiliary Call Trace Collector workstation.....	6-8
	Details on the bandwidth requirements	6-9
	Possible consequences of insufficient bandwidth.....	6-10
	Determining total bandwidth requirements for 5620 SAM-managed networks	6-10
6.10	Network latency considerations	6-11
	Common geographical location of 5620 SAM workstations	6-12
	Optimizing throughput between 5620 SAM workstations	6-12
	Additional 5620 SAM Database throughput optimizations.....	6-14
6.11	Network reliability considerations	6-14
	Reliability between 5620 SAM components	6-14
	5620 SAM Server to NE network reliability	6-15
6.12	GNE, Alcatel-Lucent OmniSwitch, 7250 SAS, Telco T5C, 9471 MME, eNodeB, and 5780 DSC considerations	6-15

7 — Scaling 7-1

7.1	Scaling guidelines	7-2
7.2	Scaling guidelines for 5620 SAM OSS Clients	7-3
	5620 SAM OSS Clients using JMS.....	7-3
	5620 SAM 3GPP OSS Client	7-4
7.3	Scaling guidelines for statistics collection	7-4
	Statistics collection definitions	7-4
	Determining the number of statistics records that will be collected	7-5
	Performance statistics.....	7-5
	Performance statistics collection and network latency	7-6
	Accounting statistics.....	7-6
	5620 SAM Database hardware platform requirements.....	7-7
	Simultaneous collection of performance and accounting statistics records	7-8
	Determining the number of performance and accounting statistics records being collected by 5620 SAM	7-8
7.4	Scaling guidelines for scheduled tests (STM)	7-8
	Guidelines for maximizing STM test execution:	7-10
	Lightweight STM test configuration	7-11
	Accounting file STM test configuration	7-11
	Examples of STM test configuration	7-11
	Factors impacting the number of elemental tests that can be executed in a given time frame.....	7-12
	Possible consequences of exceeding the capacity of the system to perform tests	7-13
	Skipped tests:	7-13
	Failed tests (time-out):	7-13
	Disk space requirements for STM test results:.....	7-13
7.5	Scaling guidelines for call trace	7-14
	Disk space requirements for Call Trace and Debug Trace	7-14

8 —	Security	8-1
8.1	Securing 5620 SAM	8-2
8.2	Operating system installation for 5620 SAM workstations	8-2
	Required Solaris services.....	8-2
8.3	5620 SAM software installation	8-3
8.4	5620 SAM network element communication	8-3
8.5	5620 SAM and firewalls.....	8-3
8.6	Ports required for firewalls.....	8-5
8.7	FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network	8-11
8.8	Firewall and NAT rules	8-12
	5620 SAM Server firewall and NAT rules	8-12
	5620 SAM Database firewall and NAT rules.....	8-17
	5620 SAM Auxiliary Server firewall and NAT rules	8-18
	5620 SAM Server to delegate workstation	8-22
	5620 SAM Client to managed network communications	8-22
9 —	Deploying 5620 SAM with multiple network interfaces/IP addresses	9-1
9.1	Deploying 5620 SAM with multiple network interfaces/IP addresses	9-2
9.2	5620 SAM Server multiple IP addresses deployment scenarios.....	9-2
9.3	5620 SAM Auxiliary Statistics Collector multiple IP addresses deployment scenarios	9-3
9.4	5620 SAM Auxiliary Call Trace Collector multiple IP addresses deployment scenarios	9-4
9.5	Using Network Address Translation	9-7
9.6	Configuring 5620 SAM Server to utilize multiple network interfaces	9-9
9.7	Use of hostnames for the 5620 SAM Client	9-9

List of figures

Figure 1 Home icon	xii
Figure 2-1 5620 SAM standalone deployment - collocated SAM Server/Database configuration.....	2-3
Figure 2-2 5620 SAM standalone deployment - distributed 5620 SAM Server and 5620 SAM Database configuration.....	2-3
Figure 2-3 5620 SAM standalone deployment - collocated 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary Call Trace Collector installed.....	2-3
Figure 2-4 5620 SAM standalone deployment - distributed 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary workstations installed	2-4
Figure 2-5 5620 SAM collocated Server/Database redundancy deployment	2-8
Figure 2-6 5620 SAM distributed Server/Database redundancy deployment in a geographically redundancy setup.....	2-8
Figure 2-7 5620 SAM distributed Server/Database redundancy deployment with redundant 5620 SAM Auxiliaries that crosses geographically boundaries.....	2-10
Figure 8-1 Firewalls and 5620 SAM standalone deployments.....	8-4
Figure 8-2 Firewalls and 5620 SAM redundant deployments	8-4
Figure 9-1 Collocated 5620 SAM Server/Database deployment with multiple network interfaces	9-5
Figure 9-2 Distributed 5620 SAM Server/Database deployment with multiple network interfaces	9-6
Figure 9-3 5620 SAM Server deployments with NAT between the Server and the managed network	9-7
Figure 9-4 NAT'd 5620 SAM Server deployment with IP Address communication.....	9-8
Figure 9-5 NAT'd 5620 SAM Server deployment with Name Resolution based communication	9-8
Figure 9-6 5620 SAM deployment with NAT	9-9

List of tables

Table 1 5620 SAM customer documentation suite	ix
Table 2 Documentation conventions	xiii
Table 3 Bits and bytes conventions	xiv
Table 3-1 5620 SAM operating system support summary	3-3
Table 4-1 5620 SAM x86 minimum collocated platforms.....	4-3
Table 4-2 5620 SAM x86 minimum distributed platforms	4-4
Table 4-3 5620 SAM SPARC Solaris minimum collocated platforms	4-4
Table 4-4 5620 SAM SPARC Solaris minimum distributed platforms.....	4-5
Table 4-5 Scaling limits for collocated platforms.....	4-5
Table 4-6 5620 SAM Auxiliary platforms.....	4-6
Table 4-7 5620 SAM Client Delegate Workstations hardware platform requirements.....	4-7
Table 4-8 5620 SAM GUI hardware platform requirements.....	4-8
Table 4-9 SAN Mount Points and performance requirements	4-11

Table 6-1 5620 SAM collocated Server/Database bandwidth requirements	6-3
Table 6-2 5620 SAM distributed Server/Database bandwidth requirements	6-3
Table 6-3 Additional bandwidth requirements for accounting statistics collection.	6-4
Table 6-4 Additional bandwidth requirements for performance statistics collection.	6-5
Table 6-5 Additional bandwidth requirements for performance management statistics collection.	6-5
Table 6-6 Additional bandwidth requirements for file accounting STM results collection logToFile method.	6-5
Table 6-7 Additional bandwidth requirements for call trace collection.	6-6
Table 6-8 5620 SAM Server to network bandwidth requirements	6-8
Table 7-1 5620 SAM Release 9.0 R5 scalability limits	7-2
Table 7-2 Network element maximums and equivalency	7-3
Table 7-3 JMS durable messaging rates	7-4
Table 7-4 3GPP OSS JMS messaging rates	7-4
Table 7-5 Maximum number of performance statistics records processed on a 5620 SAM Server	7-5
Table 7-6 Maximum number of accounting statistics records to be processed by a 5620 SAM Server workstation	7-7
Table 7-7 5620 SAM Database workstation hardware requirements for a distributed configuration	7-7
Table 7-8 Maximum number of STM elemental tests	7-9
Table 7-9 Disk space requirements for trace data.	7-14
Table 8-1 5620 SAM firewall requirements	8-6
Table 8-2 SNMP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network	8-12
Table 8-3 Telnet / FTP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network	8-13
Table 8-4 SSH / SFTP / SCP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network	8-13
Table 8-5 7250 SAS or Telco T5C Firewall rules for traffic between the 5620 SAM Server(s) and the managed network	8-13
Table 8-6 Other Firewall rules for traffic between the 5620 SAM Server(s) and the managed network	8-14
Table 8-7 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Client(s) (GUI/OSS)	8-14
Table 8-8 5620 SAM Server interface to Client firewall rules for setups with redundant 5620 SAM Servers	8-15
Table 8-9 5620 SAM Server-to-Server firewall rules for setups with redundant 5620 SAM Servers	8-15
Table 8-10 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Auxiliary Server(s)	8-15
Table 8-11 Additional firewall rules required to allow services on the 5620 SAM client(s) to communicate with the 5620 SAM Server if NAT is used.	8-16
Table 8-12 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Database Server(s)	8-16
Table 8-13 Firewall rules for setups with redundant 5620 SAM Servers.	8-16
Table 8-14 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Auxiliary Server(s).	8-17
Table 8-15 Firewall rules for traffic coming into the 5620 SAM Database Server(s) from the 5620 SAM Server(s) and 5620 SAM Auxiliary Server(s)	8-17

Table 8-16 Firewall rules for traffic between the 5620 SAM Database Servers (redundant only)	8-17
Table 8-17 SNMP Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network	8-18
Table 8-18 SSH / Telnet Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network.....	8-18
Table 8-19 SNMP FTP Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network	8-19
Table 8-20 SNMP Firewall rules for traffic coming into the 5620 SAM Auxiliary Call Trace Server(s) from the Managed Network	8-19
Table 8-21 Call Trace Data Firewall rules for traffic coming into the 5620 SAM Auxiliary Call Trace Server(s) from the Managed Network	8-19
Table 8-22 Firewall rules for OSS Client communication to the 5620 SAM Auxiliary Server(s)	8-20
Table 8-23 Firewall rules for inter process communication on the 5620 SAM Auxiliary Server(s).....	8-20
Table 8-24 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Server(s)	8-20
Table 8-25 Firewall rules for setups with redundant 5620 SAM Servers	8-21
Table 8-26 Additional Firewall rules required to allow services on the 5620 SAM client(s) to communicate with the 5620 SAM Auxiliary(s) if NAT is used on the Auxiliary Server(s).....	8-21
Table 8-27 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Database Server(s)	8-21
Table 8-28 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Server(s)	8-22
Table 8-29 Firewall rules for traffic between redundant 5620 SAM Auxiliary Statistics Collector Servers.	8-22
Table 8-30 Firewall rules for traffic between redundant 5620 SAM Auxiliary Call Trace Collector Servers.	8-22
Table 8-31 Firewall rules for traffic between the 5620 SAM Client and the 5780 DSC	8-23
Table 8-32 Firewall rules for traffic between the 5620 SAM Client and the 9471 MME.....	8-23
Table 8-33 Firewall rules for traffic between the 5620 SAM Client and the eNodeB NEM.....	8-23
Table 8-34 Firewall rules for traffic between the 5620 SAM Client and GNEs.....	8-23
Table 8-35 Firewall rules for traffic between the 5620 SAM Client and 9500 MPR NetO.....	8-23
Table 8-36 Firewall rules for traffic between the 5620 SAM Client and Omni Switches	8-24

1 — *Introduction*

- 1.1 Overview 1-2**
- 1.2 Purpose 1-2**
- 1.3 Intended audience 1-2**
- 1.4 Document changes 1-2**

1.1 Overview

The *5620 SAM Planning Guide* details the following aspects of the Alcatel-Lucent 5620 SAM product:

- Product deployment overview
- Supported operating systems specifications
- Hardware platform requirements
- Network requirements
- Scaling guidelines
- Workstation configuration
- Firewall information

1.2 Purpose

This document consolidates the technical information related to the deployment of the Alcatel-Lucent 5620 SAM Release 9.0 product. This document does not focus on the functionality offered by 5620 SAM Release 9.0 but instead presents the reader with pre-installation information required to plan a successful deployment.

The *5620 SAM Planning Guide* is not a comprehensive list of technologies supported or not supported by 5620 SAM or the platforms hosting it. The Alcatel-Lucent NSM Product Group should be consulted for clarification when uncertainty exists.

1.3 Intended audience

This document is intended for network engineers, planners and IT staff who are familiar with the functionality of the 5620 SAM and are planning a product deployment.

1.4 Document changes

This section highlights the key differences between this release of the *5620 SAM Planning Guide* and the *5620 SAM Planning Guide*, Release 8.0. Minor differences between the documents, such as updating release version references, are not listed.

- Removal of support of SAM Server and SAM database on Windows based platforms
- Removal of support of 2 CPU based workstations for SAM Server and SAM Database
- Removal of support of SPARC T-Series CPU based servers
- Update Oracle Database version
- Support for HP based servers running Solaris added
- Added SAM Supervisor information
- Firewall ports added for NEM, SAM Supervisor, and Auxiliary Servers
- Firewall ports modified for MME and DSC
- Update minimum memory requirements

- Single 73GB disk installations no longer supported
- Increased memory requirements to support 3GPP
- Refined SAN requirements
- Update maximum number of STM results that can be stored in the SAM Database
- Update supported NAT configurations - removed support for NAT between servers running 5620 SAM Server, SAM Database, and Auxiliary Servers
- Firewall ports added for NEtO
- Increased scaling limits for 7210, 9500, eNodeB and Omni 6000 series NE types
- Firewall ports updated for SAM Server and Auxiliary Servers

2 — *Product deployment overview*

- 2.1 5620 SAM architecture 2-2**
- 2.2 5620 SAM Auxiliary Statistics Collector 2-5**
- 2.3 5620 SAM Auxiliary Call Trace Collector 2-5**
- 2.4 5620 SAM Client Delegate 2-6**
- 2.5 5620 SAM key technology overview 2-6**
- 2.6 Redundancy architecture 2-7**
- 2.7 Redundancy deployment considerations for 5620 SAM 2-11**

2.1 5620 SAM architecture

Five types of platforms can be present in a 5620 SAM Release 9.0 deployment:

- 5620 SAM GUI Client workstation(s)
- 5620 SAM GUI Client Delegate workstation(s)
- 5620 SAM Server
- 5620 SAM Auxiliary (Statistics Collector and Call Trace Collector)
- 5620 SAM Database

5620 SAM Release 9.0 supports co-location of the 5620 SAM Server and 5620 SAM Database software on a single workstation when it runs the Solaris operating system.

5620 SAM Release 9.0 also supports a distributed deployment, whereby the 5620 SAM Server and the 5620 SAM Database software components are installed on two different workstations.

5620 SAM Release 9.0 supports the distribution of statistics collection and the collection of call trace information. A 5620 SAM Auxiliary can be configured for statistics collection or for call trace collection. It cannot be configured to perform both functions.

5620 SAM Release 9.0 supports redundancy of the 5620 SAM Server, 5620 SAM Database, and 5620 SAM Auxiliary workstations. This can be achieved with the 5620 SAM Server and Database being in a collocated or distributed configuration. The 5620 SAM Auxiliary can also be installed in a redundant configuration, but cannot be collocated on the same workstation with a 5620 SAM Server or 5620 SAM Database.

A 5620 SAM Auxiliary Statistics Collector must be installed on an independent workstation to reduce the burden of statistics handling from the 5620 SAM Server. The 5620 SAM Auxiliary Statistics Collector workstation can only be configured in a 5620 SAM distributed deployment.

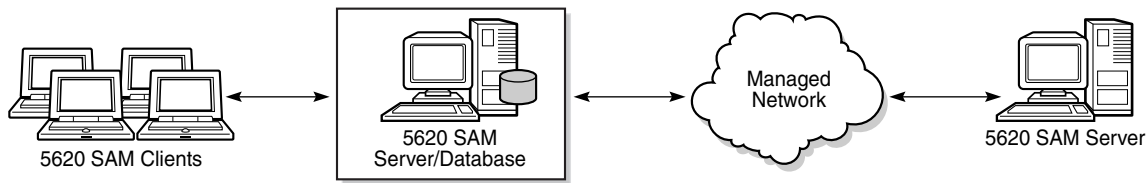
A 5620 SAM Auxiliary Call Trace Collector must be installed on an independent workstation to collect the call trace information from eNodeB network elements. Up to two active 5620 SAM Auxiliary Call Trace Collector workstations can be installed to scale the collection of call trace information. Each active 5620 SAM Auxiliary Call Trace Collector workstation can be assigned to a redundant workstation. Call trace information is synchronized between the redundant pairs. The 5620 SAM Auxiliary Call Trace Collector workstations can be configured in either a 5620 SAM distributed or collocated deployment.

More details on redundancy in 5620 SAM can be found in [section 2.6](#)

5620 SAM Release 9.0 supports IPv4 and IPv6 connectivity between the 5620 SAM Server/Auxiliary to the managed network. Connectivity between the 5620 SAM components uses IPv4 only.

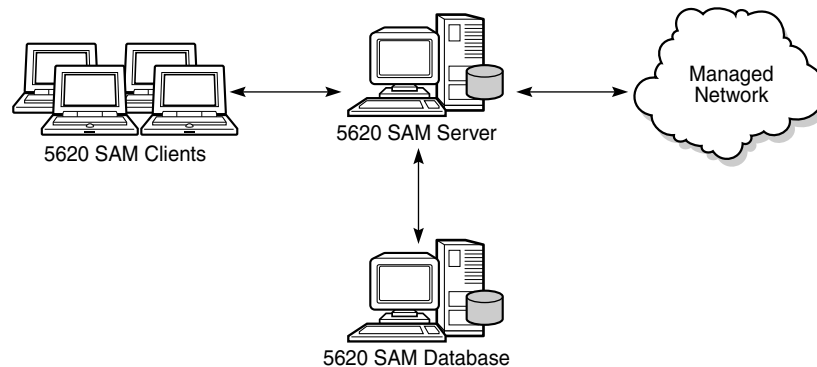
A Network element can only be managed by one 5620 SAM standalone or redundant deployment. Having multiple 5620 SAM deployments managing the same network element is not supported, and will cause unexpected behavior.

The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database platforms are collocated.

Figure 2-1 5620 SAM standalone deployment - collocated SAM Server/Database configuration

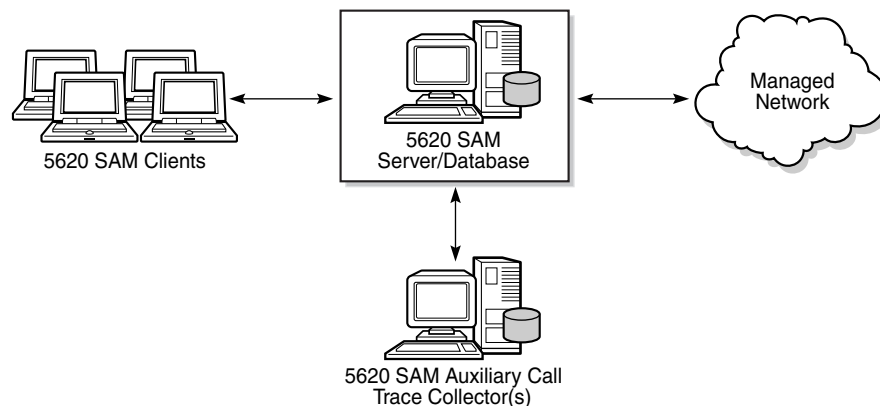
22675

The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database platforms are not collocated.

Figure 2-2 5620 SAM standalone deployment - distributed 5620 SAM Server and 5620 SAM Database configuration.

22674

The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database platforms are collocated and a 5620 SAM Auxiliary Call Trace Collector is installed. The 5620 SAM Auxiliary Statistics Collector is not supported in this configuration.

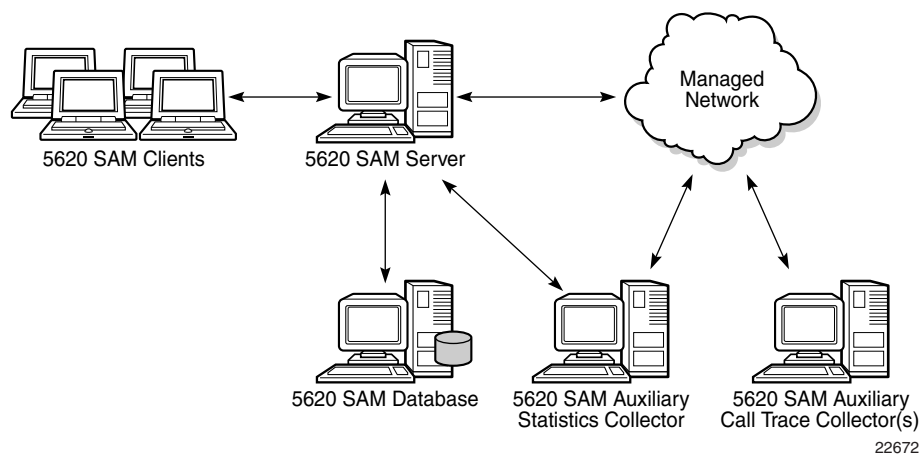
Figure 2-3 5620 SAM standalone deployment - collocated 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary Call Trace Collector installed

22673

The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database platforms are in a distributed deployment and 5620 SAM Auxiliaries are installed. In this configuration there can be a single 5620 SAM Auxiliary Statistics Collector workstation or it could be configured redundant, and there can be one or two 5620 SAM Auxiliary Call Trace Collector workstations collecting call trace data from the network.

5620 SAM standalone deployment – distributed 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary workstations installed

Figure 2-4 5620 SAM standalone deployment - distributed 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary workstations installed



5620 SAM Server, 5620 SAM Auxiliary Statistics Collector, 5620 SAM Auxiliary Call Trace Collector and 5620 SAM Database software must be installed on workstations running the same Solaris operating system.

The 5620 SAM Server, 5620 SAM Auxiliary Statistics Collector, and 5620 SAM Database can run on Oracle based SPARC servers or x86 Intel, and x86 AMD based Oracle and HP workstations. The 5620 SAM Auxiliary Call Trace Collector can only run on an x86 Intel or x86 AMD based Oracle and HP workstations. In a redundant configuration, the workstation architecture of the redundant pair must match. In the x86 case, CPU type (Intel or AMD) of the Oracle or HP x86 must match as well.

For example, a 5620 SAM Server can be installed on an Oracle x86 AMD workstation, while a 5620 SAM Database can be installed on an Oracle SPARC workstation. Their redundant pair must be Oracle x86 AMD and Oracle SPARC respectively

5620 SAM Client software may be installed on workstations running different operating systems from the 5620 SAM Server, 5620 SAM Auxiliary, and 5620 SAM Database. The 5620 SAM Client can be installed on Solaris or Windows.

All 5620 SAM workstations in the 5620 SAM management complex must maintain consistent and accurate time. It is recommended that NTP be used to accomplish this requirement.

2.2 5620 SAM Auxiliary Statistics Collector

5620 SAM Release 5.0 introduced the concept of the 5620 SAM Auxiliary Statistics Collector workstation. This type of 5620 SAM Auxiliary collects and processes performance, accounting, and performance management statistics. This option enables customers to reduce the load of statistics collection from the 5620 SAM Server while allowing for increased statistics collection capabilities. A 5620 SAM Auxiliary Statistics Collector workstation should be used when statistics collection is expected to exceed the capacity of the 5620 SAM Server. Refer to chapter 4 for scalability details of the 5620 SAM Server and dimensioning of the 5620 SAM Auxiliary Statistics Collector workstation.

The 5620 SAM Auxiliary Statistics Collector workstation can be configured as preferred or reserved for a given 5620 SAM Server (Active or Standby). This allows for a redundant 5620 SAM Auxiliary Statistics Collector configuration. Only one 5620 SAM Auxiliary Statistics Collector will collect statistics at any given time. Each 5620 SAM Auxiliary Statistics Collector is installed on a separate workstation. Information on the redundancy model of the 5620 SAM Auxiliary Statistics Collector can be found in section 2.6.

The 5620 SAM Server and the 5620 SAM Auxiliary Statistics Collector must maintain consistent and accurate time. It is encouraged to use an NTP service to achieve this. An alarm will be raised if the times are not within 30 seconds. Variations in time can cause the system to stop collecting statistics prematurely.

In networks where 5620 SAM Auxiliary Statistics Collector workstations are not configured, the 5620 SAM Server handles the statistics collection. In networks where the 5620 SAM Auxiliary Statistics Collector is configured, the 5620 SAM Server will never collect statistics – regardless of the availability of the 5620 SAM Auxiliary Statistics Collector workstations. At least one 5620 SAM Auxiliary Statistics Collector workstation must be available for statistics collection to occur.

The 5620 SAM Auxiliary Statistics Collector is only supported with a distributed 5620 SAM Server and 5620 SAM Database. The 5620 SAM Server and database platforms must be running on a supported Solaris based workstation.

For Collection of statistics from eNodeB network elements, NTP should be used to synchronize the network element and the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector to ensure the statistics are successfully retrieved.

2.3 5620 SAM Auxiliary Call Trace Collector

5620 SAM Release 8.0 R5 introduced the concept of the 5620 SAM Auxiliary Call Trace Collector workstation. This type of 5620 SAM Auxiliary collects call trace information from the eNodeB network elements.

Up to two 5620 SAM Auxiliary Call Trace Collectors can be configured to collect call trace information in 5620 SAM Release 9.0, and each of those collectors can be configured to be redundant. Each 5620 SAM Auxiliary Call Trace Collector is installed on a separate workstation. Each 5620 SAM Auxiliary Call Trace Collector workstation is configured as a preferred for the 5620 SAM Active Server and as a reserved for the 5620 SAM Standby Server. This allows for a redundant 5620 SAM Auxiliary Call Trace Collector configuration. Only one of the workstations in the

5620 SAM Auxiliary Call Trace Collector redundant pair will collect the call trace information from the network elements at any given time and the call trace information is synchronized between the Preferred and Reserved pair of workstations. Information on the redundancy model of the 5620 SAM Auxiliary Call Trace Collector can be found in section [2.6](#).

The 5620 SAM Auxiliary Call Trace Collector is supported with both a collocated 5620 SAM Server and 5620 SAM Database or distributed 5620 SAM Server and 5620 SAM Database.

The 5620 SAM Server and the 5620 SAM Auxiliary Call Trace Collector workstation must maintain consistent and accurate time. It is encouraged to use an NTP service to achieve this. An alarm will be raised if the times are not within 30 seconds.

The 5620 SAM Auxiliary Call Trace Collector is only supported on an Oracle or HP x86 platform, in either a collocated or distributed 5620 SAM Server and Database configuration. The 5620 SAM Server and Database platforms must be running Solaris on either an Oracle SPARC or x86 based Oracle or HP platform.

2.4 5620 SAM Client Delegate

This option enables customers to launch multiple 5620 SAM GUI Clients from a single Solaris workstation. These GUI clients can be displayed using the X11 protocol to other Solaris desktops or native X displays. Displaying GUI clients to computers running X-emulation software is not currently supported.

The Client Delegate platform provides an option to consolidate multiple installations of the 5620 SAM GUI Client on a single Solaris workstation. Individual 5620 SAM Clients can be installed on the Client Delegate Platform. In Release 9.0, 5620 SAM Client also supports the ability for multiple users to share a single installation; however, each user must run the client with a unique UNIX Id.

Please note that on computers running Windows, only one instance of a 5620 SAM GUI Client can be running at any given time.

Information on dimensioning the 5620 SAM Client Delegate platform is given in section [4.2](#).

2.5 5620 SAM key technology overview

This section describes the key technologies used to support 5620 SAM features.

Java Virtual Machine

The 5620 SAM Server, 5620 SAM Auxiliary, 5620 SAM Database, and 5620 SAM Client applications use Java technology. The installation packages contain a Java Virtual Machine which is installed with the software. This is a dedicated Java Virtual Machine and does not conflict with other Java Virtual Machines which may be installed on the same workstation.

5620 SAM Release 9.0 uses Java Virtual Machine version 6 from Oracle.

Oracle database

The 5620 SAM Database embeds an installation of Oracle 11g Release 2 Enterprise Edition, which is installed on the 5620 SAM Database workstations. This database is used to store information about the managed network. The installation of Oracle is customized for use with the 5620 SAM application and must be dedicated to 5620 SAM. 5620 SAM database redundancy uses Oracle DataGuard, and is configured in maximum performance mode.

Alcatel-Lucent will not support any configuration deviations from the Oracle installation as performed by the 5620 SAM Database installation package, as it represents a 5620 SAM License Agreement Violation. Modifying the Oracle installation can impact system performance, stability and upgrades. Customer support agreements may be violated.

The Oracle Database is embedded with the 5620 SAM Product and because of this; Oracle requires all CPU licenses to be purchased from Alcatel-Lucent. This applies to customers with Oracle Site licenses as well.

2.6 Redundancy architecture

Redundancy between 5620 SAM Server and Database applications is used to ensure visibility of the managed network is maintained when one of the following failure scenarios occur:

- Loss of physical network connectivity between 5620 SAM Server and/or 5620 SAM Database and the managed network
- Hardware failure on workstation hosting the 5620 SAM Server and/or 5620 SAM Database software component

5620 SAM supports redundancy of the 5620 SAM Server and 5620 SAM Database components in the following workstation configurations:

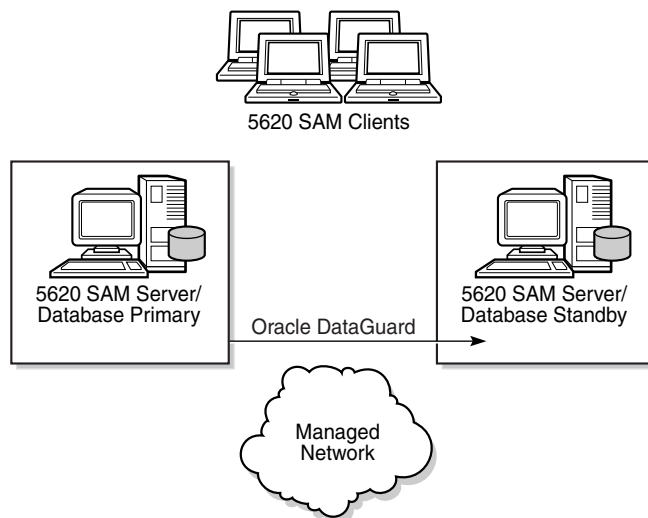
- 5620 SAM Server and 5620 SAM Database collocated and redundant (i.e. two workstations)
- 5620 SAM Server and 5620 SAM Database distributed and redundant (i.e. four workstations)

The 5620 SAM redundancy feature is only supported when the 5620 SAM Server and 5620 SAM Database software is installed on the Solaris operating system.

5620 SAM uses Oracle DataGuard configured in “maximum performance” and “Real-time apply” mode to implement the redundancy model.

The following illustrates a 5620 SAM redundant installation when the 5620 SAM Server and 5620 SAM Database components are collocated on the same Oracle or HP x86 Solaris workstation.

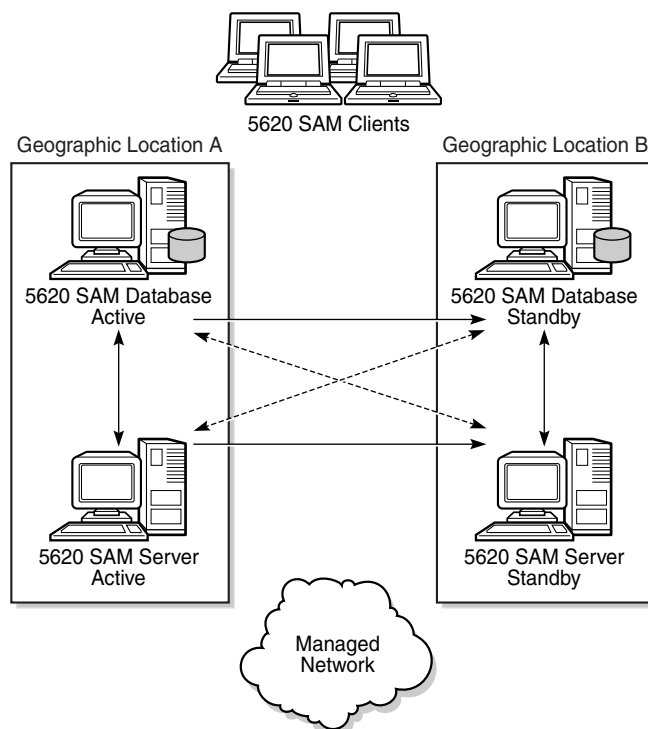
Figure 2-5 5620 SAM collocated Server/Database redundancy deployment



22671

The following illustrates a 5620 SAM redundant installation when the 5620 SAM Server and 5620 SAM Database components are located on different Solaris workstations.

Figure 2-6 5620 SAM distributed Server/Database redundancy deployment in a geographically redundancy setup.



22670

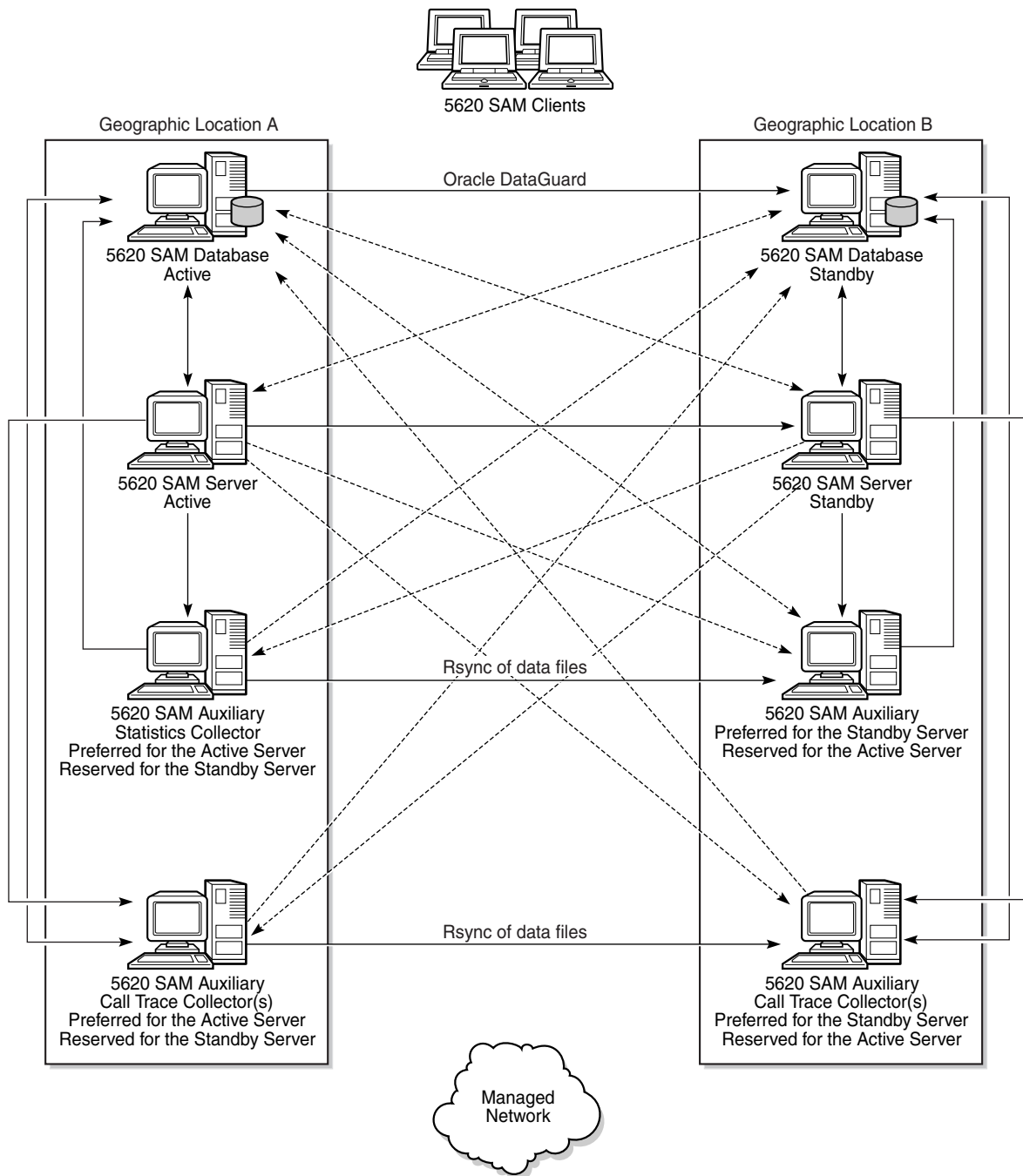
Redundancy and 5620 SAM Auxiliary workstations

In customer networks where the statistics collection requirements exceed the scalability capabilities of a 5620 SAM Server, 5620 SAM Auxiliary Statistics Collector workstations can be used. As with other high availability components, 5620 SAM Auxiliary Statistics Collector can be configured to be redundant. Each 5620 SAM Server can be configured to have one preferred and one reserved 5620 SAM Auxiliary Statistics Collector.

In customer networks where Call Trace information is being collected from eNodeB network elements, a 5620 SAM Auxiliary Call Trace Collector must be used. The 5620 SAM Auxiliary Call Trace Collector workstations can be installed in a redundant pair. Up to two 5620 SAM Auxiliary Call Trace Collector redundant pairs can be installed.

In Figure 2-7, there are workstations that are configured as 5620 SAM Auxiliary workstations. In the example where redundancy is geographic, there can be one 5620 SAM Auxiliary Statistics Collector and up to two 5620 SAM Auxiliary Call Trace Collector workstations configured in each geographic location. The Preferred/Reserved role of the 5620 SAM Auxiliary is dependant and configured on the 5620 SAM Server that is active. In both geographic locations, the 5620 SAM Server is configured such that the 5620 SAM Auxiliary in its geographic location is preferred. The 5620 SAM Auxiliary in the opposite geographic location is configured to be reserved. In this scenario, if the 5620 SAM Auxiliary for the active 5620 SAM Server were to no longer be available, the active 5620 SAM Server would use the reserved 5620 SAM Auxiliary in the opposite geographic location to collect statistics.

Figure 2-7 5620 SAM distributed Server/Database redundancy deployment with redundant 5620 SAM Auxiliaries that crosses geographically boundaries



22669

Further information about 5620 SAM redundancy can be found in the *5620 SAM User Guide*

2.7 Redundancy deployment considerations for 5620 SAM

When deploying 5620 SAM in a redundant configuration, the following items should be considered.

It is a best practice to keep the 5620 SAM Server, 5620 SAM Database, and 5620 SAM Auxiliary in the same geographic site to avoid the impact of network latency. When the 5620 SAM Database or 5620 SAM Server switches sites, the 5620 SAM auto-align functionality will ensure the SAM Server, 5620 SAM Auxiliary, and 5620 SAM Database are all aligned in the same geographic location. If the auto-align functionality is not enabled, a manual switch of the workstations is desirable.

Redundancy with collocated 5620 SAM Server/Database:

- The operating systems installed on the primary and standby 5620 SAM Server/Database machines must be of the same versions and at the same patch levels.
- The layout and partitioning of the disks containing the 5620 SAM software, the Oracle software and the database data must be identical on the active and standby 5620 SAM Server/Database machines.
- The machine which will be initially used as the active 5620 SAM Server/Database must be installed or upgraded before the machine that will initially be used as the standby.
- The workstations hosting the 5620 SAM software should be connected in a way to prevent a single physical failure from isolating the two workstations from each other.
- Workstations running the 5620 SAM Server/Database software must be configured to perform name service database lookups on the local workstation before reverting to a name service database located on the network such as NIS, NIS+, or DNS. A root user must inspect and modify the `/etc/nsswitch.conf` file to ensure that files is the first entry specified for each database listed in the file.

Redundancy with distributed 5620 SAM Server and 5620 SAM Database:

- The operating systems installed on the primary and standby 5620 SAM Server as well as the primary and standby 5620 SAM Database machines must be of the same versions and at the same patch levels.
- The layout and partitioning of the disks containing the 5620 SAM software, the Oracle software and the database data must be identical on the primary and standby 5620 SAM Database machines.
- The machines which are intended to be used as primary 5620 SAM Server and 5620 SAM Database should be installed on the same LAN as one another with high quality network connectivity.
- The machines which are intended to be used as standby 5620 SAM Server and standby 5620 SAM Database should be installed on the same LAN as one another with high quality network connectivity.

- The pair of workstations to be used as active 5620 SAM Server and 5620 SAM Database should be connected to the pair of workstations to be used as standby 5620 SAM Server and 5620 SAM Database in a way that will prevent a single physical failure from isolating the two workstation pairs from each other.
- Workstations running the 5620 SAM Server and 5620 SAM Database software must be configured to perform name service database lookups on the local workstation before reverting to a name service database located on the network such as NIS, NIS+, or DNS. A root user must inspect and modify the `/etc/nsswitch.conf` file to ensure that *files* is the first entry specified for each database listed in the file.

Redundancy with distributed 5620 SAM Server and 5620 SAM Database and 5620 SAM Auxiliary workstations:

In addition to the rules stated above for distributed 5620 SAM Server and 5620 SAM Database, the following rules apply:

- The operating systems installed on the 5620 SAM Auxiliary workstations must be of the same versions and patch levels as the 5620 SAM Server and 5620 SAM Database workstations.
- 5620 SAM Auxiliary workstations are intended to be on the same high availability network as the 5620 SAM Server and 5620 SAM Database workstations. 5620 SAM Auxiliary workstations are intended to be geographically collocated with the Active and Standby locations of the 5620 SAM Server and 5620 SAM Database workstations.
- Workstations running the 5620 SAM Auxiliary software must be configured to perform name service database lookups on the local workstation before reverting to a name service database located on the network such as NIS, NIS+, or DNS. A root user must inspect and modify the `/etc/nsswitch.conf` file to ensure that *files* is the first entry specified for each database listed in the file.

3 — *Operating systems specifications*

- 3.1 Solaris (Oracle and HP platforms) 3-2**
- 3.2 Microsoft Windows 3-2**
- 3.3 Operating system summary 3-3**
- 3.4 5620 SAM Client or Delegate software requirements 3-3**

3.1 Solaris (Oracle and HP platforms)

5620 SAM Release 9.0 is supported on Solaris 10 10/08 (Update 6) or later for the 5620 SAM Server, 5620 SAM Auxiliary, 5620 SAM Database and 5620 SAM Client. 5620 SAM Release 9.0 requires the following minimum base Solaris version (not updated using a Solaris Maintenance Update):

- Solaris 10 - 10/08 S10S_u6
- Solaris 10 - 05/09 S10S_u7
- Solaris 10 - 10/09 S10S_u8 (requires patch 142901-09 or newer)
- Solaris 10 - 09/10 S10S_u9

The Solaris support of the 5620 SAM Release 9.0 is applicable to SPARC platforms provided by Oracle and x86 AMD and Intel platforms provided by Oracle and HP only, with the exception of 5620 SAM Auxiliary Call Trace Collectors and the 5620 SAM-O 3GPP Interface that only operate on Oracle or HP x86 Intel or AMD platforms. Some systems may require specific versions of the Solaris OS. See Oracle's hardware compatibility list (HCL) on their website. 5620 SAM does not support all functionality introduced in Solaris 10 (for example zones or ZFS).

The redundancy feature of 5620 SAM is supported when the 5620 SAM Server, 5620 SAM Auxiliary and 5620 SAM Database software is installed on supported Solaris platforms. In this situation, the 5620 SAM Client software can be installed on Solaris or Windows platforms.

The Solaris operating system must be installed in 64-bit mode on workstations that will contain the 5620 SAM Server, 5620 SAM Auxiliary, 5620 SAM Database or 5620 SAM Client software. 32-bit mode is not supported.

The 5620 SAM Server, Auxiliary and Database workstation Solaris operating system must be installed in English. Multi-language Solaris is not supported.

5620 SAM can be installed in a collocated configuration, where the 5620 SAM Server and the 5620 SAM Database are installed on the same supported, Solaris based workstation.

Customers are solely responsible for securing Solaris support from Oracle for both HP and Oracle based platforms. Oracle may choose to modify Solaris support agreements for HP based platforms at any time in the future and is beyond the control of Alcatel-Lucent.

3.2 Microsoft Windows

As of 5620 SAM release 9.0, the Windows operating system is only supported for 5620 SAM Clients. The following 32-bit versions of Windows are supported:

- Windows 2000
- Windows 2003
- Windows XP Professional Edition
- Windows Vista Business/Enterprise and Ultimate
- Windows 7 Professional

The following 64-bit versions of Microsoft Windows are supported:

Windows 7 Professional

When installing the 5620 SAM Client on a Windows computer platform, ensure that there is sufficient disk space as identified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for the software.

Windows XP-SP2 will – by default – turn on the Windows Firewall functionality. This could cause difficulties with system operation. See section 8.6 for more details on specific ports that must be enabled for 5620 SAM operation.

3.3 Operating system summary

Table 3-1 summarizes the supported configurations for each of the Operating Systems supported by 5620 SAM Release 9.0.

Table 3-1 5620 SAM operating system support summary

5620 SAM application	Oracle Solaris 10	Microsoft Windows
5620 SAM Server	Supported	Not supported
5620 SAM Database		
Collocated 5620 SAM Server/Database	Supported	Not supported
5620 SAM Client	Supported	Supported
5620 SAM Auxiliary	Supported (Call Trace Collector only supported on x86)	Not supported
5620 SAM Redundancy (Server and Database)	Supported	Not supported
5620 SAM Client Delegate	Supported	Not supported

3.4 5620 SAM Client or Delegate software requirements

5620 SAM clients can be launched, installed and uninstalled through a web browser (Web Launch, Install and Uninstall). To use this functionality, each client platform must have a system JRE (Java Runtime Environment) installed. The 5620 SAM web browser installer/launcher requires Java version 6.0 update 20 or greater for the system JRE. The system JRE needs to be already installed on the client platform. The system JRE is only used for the SAM client web browser installer/launcher, it is not required for installing, launching or running the 5620 SAM client when the web browser launch is not used.

5620 SAM 9.0 introduces support for SAM Supervision that is launched from the 5620 SAM Client in a web browser. SAM Supervision has the following requirements:

- Adobe Flash Player browser plug-in

and one of the following Internet Browsers

- 32-bit Microsoft Internet Explorer 6 or 8
- Firefox 3.5.9

Additional Web Browsers may function with SAM Supervision but they are not supported by Alcatel-Lucent.

4 — *Hardware platform requirements*

- 4.1 Hardware platform requirements overview 4-2**
- 4.2 Minimum hardware platform requirements 4-2**
- 4.3 5620 SAM-O 3GPP Interface 4-7**
- 4.4 5620 SAM GUI Client hardware platform requirements 4-8**
- 4.5 Determining hardware platform requirements for larger networks 4-8**
- 4.6 Solaris workstation disk configuration 4-9**

4.1 Hardware platform requirements overview

This section defines the hardware platform requirements for successfully running the 5620 SAM Release 9.0 application. Following these platform guidelines is necessary to ensure the 5620 SAM Release 9.0 application performs adequately.

For new installations, Alcatel-Lucent encourages the use of Oracle x86 AMD or Oracle x86 Intel based workstations. Their performance exceeds similar sized SPARC workstations and have a more attractive price point.

5620 SAM 9.0 is also supported on HP supplied Intel based x86 workstations.

The following platforms are not supported:

- All Oracle UltraSPARC T-series based blades and servers
- Oracle SPARC Enterprise M-Series Servers
- AMD, and Intel systems by vendors other than Oracle or HP
- SPARC systems by vendors other than Oracle

For optimal disk I/O performance, the read cache must be enabled for each disk, through Solaris. Specific HBA controllers may be required for certain platforms to ensure that the read cache can be enabled. The platform manufacturer should be consulted to determine the correct HBA controller to allow the creation of the correct number of volumes and enable the read cache.

The 5620 SAM for redundant installations requires matching workstations for the active and inactive platforms. It is acceptable to have different platforms for the Server, Database, and auxiliaries but their redundant platform must be the same.

Applications that are not sanctioned by Alcatel-Lucent should not be running on any of the 5620 SAM server, auxiliary or database workstations. Alcatel-Lucent reserves the right to remove any application from workstations running 5620 SAM components that are suspected of causing issues.

The hardware platforms do not support running applications that are not specifically identified for that platform. For instance, a 5620 SAM client is not supported on the hardware platform for a distributed or collocated 5620 SAM Server as there is a significant memory requirement for the 5620 SAM client that will impact the behavior of the 5620 SAM Server platform.

In order to support running a 5620 SAM GUI Client on a 5620 SAM server, a minimum of 16 GB RAM is required for a 5620 SAM Server in a distributed configuration, and 24 GB RAM is required for a 5620 SAM Server/Database in a collocated configuration.

5620 SAM does not support any form of virtualization.

4.2 Minimum hardware platform requirements

The following tables specify the minimum hardware platform requirements necessary to successfully operate the 5620 SAM Release 9.0 application. These minimum hardware platform requirements apply when the network being managed does not exceed any of the characteristics listed in the table [4-1](#).

The minimum platform requirements also represent the smallest configurations suitable for lab evaluations and demonstrations of the 5620 SAM Release 9.0 product.

For installation purposes, a DVD-ROM is required. For easier management of the system, a graphics card is recommended.

Minimum hardware platform requirements for Solaris

Table 4-1 lists the minimum hardware platform requirements for deployments of the 5620 SAM Release 9.0 product on the SPARC and x86 Solaris operating system.

Alcatel-Lucent continues to support deployments of 5620 SAM Release 9.0 on SPARC Solaris platforms from Oracle which are based on the UltraSPARC III Cu, UltraSPARC IIIi, UltraSPARC IV, and UltraSPARC IV+.

The minimum collocated platforms (for both x86 and SPARC) will deliver acceptable performance in situations in small network which are expected to be relatively static. If the rate of changes in the network or if the rate of transactions through the OSS application(s) are expected to exceed a few changes per second, the collocated minimum platform specified below will not be sufficient to deliver adequate performance. In that case, the distributed minimum platform is recommended.

Customers are solely responsible for securing Solaris support from Oracle for both HP and Oracle based platforms. Oracle may choose to modify Solaris support agreements for HP based platforms at any time in the future and is beyond the control of Alcatel-Lucent.

Oracle or HP x86 hardware configuration:

Table 4-1 5620 SAM x86 minimum collocated platforms

For networks not exceeding: <ul style="list-style-type: none"> • 675 MDAs • 1000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 1000 elemental STM tests every 10 minutes • 50,000 performance or 100,000 accounting statistics records every 15 minutes 	
5620 SAM application	Configuration
5620 SAM Server and Database (Collocated)	2 * x86 Dual Core or 1 * x86 Quad Core 12 GB RAM minimum. 16GB RAM is recommended (24 GB RAM is recommended for Intel x86 based platforms) 4 SAS disk drives of size 146 GB is required for performance and storage capacity. Example platforms: Sun Fire X4200 or X4140 or X4170 Server / Proliant DL380 G6

Table 4-2 5620 SAM x86 minimum distributed platforms

For networks not exceeding: <ul style="list-style-type: none"> • 1875 MDAs • Maximum of 5,000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 2000 elemental STM tests every 10 minutes • 150,000 performance or 200,000 accounting statistics records every 15 minutes OR <ul style="list-style-type: none"> • 1275 MDAs • Maximum of 5,000 GNEs • 25 simultaneous 5620 SAM Clients (GUI or OSS) • 2000 elemental STM tests every 10 minutes • 150,000 performance or 200,000 accounting statistics records every 15 minutes 	
5620 SAM application	x86 architecture
5620 SAM Server	2 * x86 Dual Core or 1 * x86 Quad Core 12 GB RAM minimum. 16GB RAM is recommended (24 GB RAM is recommended for Intel x86 based platforms). 2 SAS disk drives of at least size 73 GB each in size Example platform: Sun Fire X4200 or X4140 or X4170 Server / Proliant DL380 G6
5620 SAM Database	2 * x86 Dual Core or 1 * x86 Quad Core 8 GB RAM minimum. 12 GB is recommended 4 SAS disk drives of size 146 GB is required for performance and storage capacity Example platform: Sun Fire X4200 or X4140 or X4170 Server / Proliant DL380 G6

Oracle SPARC hardware configuration:

Table 4-3 5620 SAM SPARC Solaris minimum collocated platforms

For networks not exceeding: <ul style="list-style-type: none"> • 675 MDAs • 1000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 800 elemental STM tests every 10 minutes • 50,000 performance or 100,000 accounting statistics records every 15 minutes 	
5620 SAM application	UltraSPARC III Cu/IIIi/IV/IV+ architecture
5620 SAM Server and Database (Collocated)	4 * CPU @ 1 GHz or faster 12 GB RAM minimum. 16 GB RAM is recommended 4 SCSI disk drives of at least 73 GB in size is required for performance and storage capacity Example platform: Sun Fire v440/v445 Server or Sun Fire v490 Server

Table 4-4 5620 SAM SPARC Solaris minimum distributed platforms

For networks not exceeding: <ul style="list-style-type: none"> • 1875 MDAs • Maximum of 3,000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 1000 elemental STM tests every 10 minutes • 100,000 performance or 200,000 accounting statistics records every 15 minutes OR <ul style="list-style-type: none"> • 1275 MDAs • Maximum of 3,000 GNEs • 25 simultaneous 5620 SAM Clients (GUI or OSS) • 1000 elemental STM tests every 10 minutes • 100,000 performance or 200,000 accounting statistics records every 15 minutes 	
5620 SAM application	Ultra SPARC III Cu/IIIi/IV/IV+ architecture
5620 SAM Server	4 * CPU @ 1 GHz or faster 12 GB RAM minimum. 16 GB RAM is recommended 2 SCSI disk drives that are at least 73 GB each in size Example platform: Sun Fire v440/v445 Server/Sun or Fire v490 Server
5620 SAM Database	4 * CPU @ 1 GHz or faster 8 GB RAM minimum. 16 GB RAM is recommended. 4 SCSI disk drives of at least 73 GB in size is required for performance and storage capacity Example platform: Sun Fire v440/v445 Server/Sun or Fire v490 Server

The minimum hardware platforms above are also applicable in situations where the 5620 SAM application is installed in a redundant configuration.

Scaling limits for collocated platforms

Collocated platforms have been capped at the maximums described in table 4-5. Higher numbers may be achievable, but Alcatel-Lucent will only support the stated maximums. In the event that higher number of simultaneous 5620 SAM Clients is desired, the number of equivalent MDAs can be reduced. Note that all stated maximums may not be achievable simultaneously.

Table 4-5 Scaling limits for collocated platforms

Scaling parameter	Maximum
Number of MDAs	1,875
Number of Simultaneous 5620 SAM Clients (GUI or OSS)	5
Number of SAPs	600,000
Number of OAM tests per 10 minute interval	1,000
Performance Statistics per 15 minute interval	50,000
Accounting statistics per 15 minute interval	200,000

Minimum hardware platform requirements for 5620 SAM Auxiliary workstations

The 5620 SAM Auxiliary Call Trace Collector is limited to only the x86 architecture

Table 4-6 5620 SAM Auxiliary platforms

Architecture	Supported 5620 SAM Auxiliary type	Configuration
Oracle SPARC	Statistics Collector	4 * CPU @ 1.5 GHz or faster 8 GB RAM minimum. 16GB RAM is recommended. 4 SCSI disk drives of at least 73 GB in size (Multiple disks can be used to stripe the drives used to store files for the logToFile method of statistics collection) Example platform: Sun Fire v440/v445 Server/Sun Netra 440
Oracle or HP x86	Statistics Collector	2 * x86 Dual Core or 1 * x86 Quad Core 8 GB RAM minimum. 16GB RAM is recommended. 4 SAS disk drives of at least 73 GB each in size: Statistics collector uses 2 disks in a striped configuration to store files for the logToFile method of statistics collection. Example platform: Sun Fire X4200 or X4140 or X4170 Server / Proliant DL380 G6
Oracle or HP x86	Call Trace Collector	2 * x86 Quad Core Intel based HT 24 GB RAM minimum. 8 SAS disk drives of at least 146 GB each in size: Call Trace collector uses a striped configuration to store call trace files and debug trace files. 4 SAS disk drives of at least 146 GB each in size can be used, however, scale and performance will be reduced with this configuration Example platform: Sun Fire X4170 M2 or X4270 M2 Server / Proliant DL380 G6

When a 5620 SAM Statistics Auxiliary Workstation is installed, the 5620 SAM Database workstation is required to have a minimum 16 GB RAM to accommodate the additional Oracle database sessions.

Hardware platform requirements for 5620 SAM Client Delegate workstations

5620 SAM Release 9.0 allows multiple GUI clients to be installed on a single Oracle SPARC, Oracle x86, or HP x86 workstation running Solaris. This option enables customers to launch multiple 5620 SAM GUI Clients from a single Solaris workstation. These GUI clients can be displayed using a Citrix Client/Server, the X11 protocol to other Solaris desktops, or native X displays.

The Client Delegate platform provides an option to consolidate multiple installations of the 5620 SAM GUI Client on a single Solaris workstation or the option of installing one instance of the 5620 SAM GUI client run by many users (with unique Unix accounts). Regardless of the method of the client installation, the hardware platform requirements per client are the same.

Additional memory for each 5620 SAM Client will be required for management of the network elements described in section 6.12.

Additional memory for each 5620 SAM Client will also be required for a Web Browser if SAM Supervisor is to be used.

The 5620 SAM Client Delegate configuration is only supported for Oracle SPARC, Oracle x86, or HP x86 workstations running Solaris. Platforms running Windows can only run one instance of a 5620 SAM GUI Client at any given time. Table 4-7 describes platforms requirements for this type of workstation.

Table 4-7 5620 SAM Client Delegate Workstations hardware platform requirements

Number of simultaneous 5620 GUI Clients on platform	Number of CPU cores required	Amount of RAM required	Example platforms
15	4	16 GB	Sun Fire X4200 or X4140 or X4170 Server / Proliant DL380 G6 or Sun Fire v440/v445 Server / Netra 440
30	8	32 GB	Sun Fire X4140 or X4170 Server / Proliant DL380 G6 or Sun Fire v490 Server

For situations where more than 30 simultaneous GUI sessions are required, Alcatel-Lucent recommends deploying multiple 5620 SAM Client Delegate workstations.

Displaying GUI clients to computers running X-emulation software is not currently supported. In cases where the GUI client is to be displayed to a PC computer running Windows, Alcatel-Lucent supports installing the GUI client directly on the PC.

5620 SAM supports using Citrix for remote display of 5620 SAM Clients. Supporting Citrix on the delegate platform will require extra system resources that will need to be added to those that are required by the 5620 SAM delegate. Refer to Citrix documentation to determine the additional Citrix resource requirements. The following Citrix software has been tested:

- Citrix Server - XenApp Presentation Server 4.0 with Feature Pack 1 for Solaris x86
- Citrix Client - Version 8.50.117422 for Solaris x86

4.3 5620 SAM-O 3GPP Interface

5620 SAM-O 3GPP Interface is used by management systems that need to access 5620 SAM information collected from mobile networks. The 5620 SAM-O 3GPP Interface is supported as of 5620 SAM Release 8.0 R5. It is only available on Oracle or HP x86 platforms.

5620 SAM-O 3GPP Interface requires a separate JVM to be installed on the 5620 SAM Server, and is only supported on 5620 SAM Servers with a minimum 16 GB RAM in a distributed configuration or 5620 SAM Server/Databases with a minimum 24 GB RAM in a collocated configuration.

4.4 5620 SAM GUI Client hardware platform requirements

Alcatel-Lucent recommends 1 GB of dedicated RAM – regardless of the operating systems. In cases where other applications are running on the same platform as the 5620 SAM Client, it is important to ensure 1 GB RAM is available to the 5620 SAM Client. While the minimum required RAM can be 512 MB, performance will be diminished if network or user activity cause GUI memory growth.

Additional memory for each 5620 SAM Client will be required for web management of the network elements described in section [6.12](#).

Table [4-8](#) below provides the minimum requirement for the hardware that will host 5620 SAM GUI client software.

Table 4-8 5620 SAM GUI hardware platform requirements

5620 SAM GUI Client hardware platform requirements	
Oracle SPARC and x86 platforms	Microsoft Windows
1 CPU @ 1 GHz or higher (UltraSPARC III Cu or IIIi) 1 GB dedicated RAM 1 GB available disk space 1280*1024 Display resolution Example platform: Sun Ultra 45 Workstation	1 CPU @ 2 GHz or higher 1 GB dedicated RAM 1 GB available disk space 1280*1024 Display resolution

4.5 Determining hardware platform requirements for larger networks

5620 SAM Release 9.0 may require larger workstations in order to successfully manage networks that exceed any of the dimensions supported by the minimum hardware platforms. In order to determine workstation requirements to successfully manage larger networks, the following information is required:

- Expected number and types of Network Elements to be managed
- Expected number of MDAs in the network to be managed
- Expected number of services and SAPs in the network to be managed
- Expected number of Dynamic LSPs to be deployed in the network
- Maximum expected number of 5620 SAM Clients (GUI) simultaneously monitoring the network
- Expected number of OSS applications that will connect as clients to the 5620 SAM-O interface

- Expected number of subscribers, specifically for triple-play network deployments
- Expected statistics collection
- Expected number of STM tests
- Expected number of managed GNEs
- Whether 5620 SAM redundancy is to be utilized
- Whether NEBS compliance is required
- Whether CPAM is required
- Expected number of simultaneous Call Trace sessions
- Whether RAID 1 is required

The information above must then be sent to an Alcatel-Lucent representative who can provide the required hardware specifications.

Ensure that any projected growth in the network is taken to account when specifying the expected network dimensioning attributes. For existing 5620 SAM systems, the user may determine the number of MDAs deployed in the network using the help button on the 5620 SAM GUI. It is also possible to determine the number of statistics being handled by the system by looking at the 5620 SAM GUI's "Statistics Collection" information window. Select the "Tools", then "Statistics", then "Server Performance" Menu. List the "Statistics Collection" objects. From this list window, check the "Scheduled Polling Stats Processed Periodic" and the "Accounting Stats Processed Periodic" columns for the performance and accounting stats that your system is currently processing within the time interval defined by the collection policy (15 minutes by default).

Oracle licensing is dependent on the configuration of the 5620 SAM Database workstation required to support the scaling requirements. Extra licenses could be required for both the primary and standby 5620 SAM Database workstations.

4.6 Solaris workstation disk configuration

This section provides information on configuring workstations that will host 5620 SAM Release 9.0 software. These recommendations are specific to Solaris workstations.

Specific partition sizes and configuration procedures are available in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Solaris UFS is the required file system. 5620 SAM does not support the ZFS file system.

While Alcatel-Lucent identifies areas of the disk that are not specifically required for 5620 SAM and are partitionable for customer use, workstation resources are expected to be dedicated for 5620 SAM. As such, these "Remainder" portions of the disks should only be used for static storage purposes. Consideration should also be made to the expected growth of the network. If the "Remainder" is not to be used, then it should not be created.

For most network sizes, Alcatel-Lucent requires the use of 4 disks on workstations running the 5620 SAM Database. This disk configuration allows for better performance by distributing the database onto multiple disks. Customized disk configurations may be required for larger network deployments or where large scale statistics collection is required. Request a formal platform sizing for further details. NAS disk configurations are not supported.

A single-disk configuration greatly limits the 5620 SAM system performance, managed-network size, and data storage capacity, and is therefore only supported for lab trials.

Refer to section 7.3 for statistics collection recommendations.

In 5620 SAM upgrade scenarios, previous disk configurations may still be valid.

To alter existing disk configurations, a migration plan is available. Consult with Alcatel-Lucent personnel.

Using RAID technologies

Alcatel-Lucent supports the use of RAID 0 (striping) only on supported Solaris based workstations. Alcatel-Lucent does not recommend using software RAID 0. Alcatel-Lucent will provide disk layout and configuration details for customers requiring a Storage Array or layouts not specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*. The increased disk I/O performance offered by RAID 0 is required for a 5620 SAM database with a high rate of changes/updates. RAID 0 is also required in certain instances when using Call Trace and Statistics Auxiliaries. The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* provides details of these configurations. A RAID 0 stripe size of 512 Kbytes is required for optimal 5620 SAM disk performance. If a platform does not support a stripe size of 512 Kbytes, choose the next largest stripe size, for example, 256 Kbytes. Specifying a smaller or larger stripe size may result in degraded performance that compromises 5620 SAM network management.

Alcatel-Lucent supports the use of RAID 1 (Mirroring) only on supported Solaris based workstations. Deployments requiring increased resiliency are encouraged to use 5620 SAM platform redundancy. If RAID 1 is required, a platform providing hardware RAID 1 and that has sufficient number of disk to meet *5620 SAM Planning Guide* recommendations should be selected.

Alcatel-Lucent recommends the use of RAID 1+0 in deployments requiring the use of RAID 0 and RAID 1.



Note — Alcatel-Lucent is not responsible for installation, administration or recovery of RAID on a 5620 SAM platform.

Using SAN storage

As of 5620 SAM Release 8.0 R5, Alcatel-Lucent supports the use of SAN storage only on supported Solaris based workstations. SAN connectivity must consist of 4Gb or faster optical connections with dedicated Fiber Channel connections between the hosts and storage arrays. The SAN must be available to 5620 SAM without interruption in a low latency environment.

Refer to table 4-9 for required mount points and performance targets when using 5620 SAM with a SAN. Note that certain mount points may not be required due to deployment options. Refer to the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for required mount points based upon the type of 5620 SAM workstations deployed.

Table 4-9 SAN Mount Points and performance requirements

Mount Point	Average IOPS	Average Read (KB/s)	Peak Read (KB/s)	Average Write (KB/s)	Peak Write (KB/s)
/opt/5620sam	100	3,000	90,000	7,000	30,000
/opt/5620sam/server/xml_output	450	6,000	100,000	18,000	90,000
/opt/5620sam/auxserver/xml_output	450	6,000	100,000	18,000	90,000
/opt/5620sam/dbbackup	450	6,000	100,000	18,000	90,000
/opt/5620sam/dbbackup/staging	100	3,000	90,000	7,000	30,000
/opt/5620sam/samdb/tablespace	950	7,000	150,000	18,000	90,000
/opt/5620sam/samdb/tablespace/statstbs01	950	7,000	150,000	18,000	90,000
/opt/5620sam/samdb/redolog	450	6,000	100,000	18,000	90,000
/opt/5620sam/samdb/archivelog	100	3,000	90,000	7,000	30,000
/opt/5620sam/calltrace	1900	24,000	72,000	21,000	85,000
/opt/5620sam/debugtrace	1900	24,000	72,000	21,000	85,000
/opt/5620sam/lte	450	6,000	100,000	18,000	90,000

The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* should be consulted for recommended partition sizes.



Note — Alcatel-Lucent is not responsible for installation, administration or recovery of SANs on a 5620 SAM platform.

5 — *NE maintenance*

- 5.1 Mechanism to maintain current state of network elements 5-2
- 5.2 IP connectivity (ping) verification 5-2
- 5.3 SNMP connectivity verification 5-2
- 5.4 SNMP traps 5-3
- 5.5 SNMP trap sequence verification 5-3
- 5.6 Scheduled SNMP MIB polling 5-3
- 5.7 Network outages 5-3

5.1 Mechanism to maintain current state of network elements

5620 SAM uses several mechanisms to maintain and display the current state of the network elements it manages. These mechanisms can include:

- IP connectivity (ping) verification
- SNMP connectivity verification
- SNMP traps
- SNMP trap sequence verification
- Scheduled SNMP MIB polling

These mechanisms are built into the Alcatel-Lucent 7450, 7750, 7450, 7710, and 7705 Network Elements and the 5620 SAM network element interaction layers.

5.2 IP connectivity (ping) verification

5620 SAM can be configured to ping all network elements at a configurable interval to monitor IP connectivity. If the network element is unreachable, an alarm will be raised against the network element. Details of the alarm are the following:

- Severity: Critical
- Type: communicationsAlarm
- Name: StandbyCPMManagementConnectionDown, OutOfBandManagementConnectionDown or InBandManagementConnectionDown
- Cause: managementConnectionDown.

Ping verification is disabled by default.

5.3 SNMP connectivity verification

5620 SAM performs an SNMP communication check every 4 minutes. If 5620 SAM can not communicate via SNMP with a network element, 5620 SAM will raise a communications alarm against that network element. 5620 SAM will also color the network element red on the map to indicate the communication problem. 5620 SAM will clear the alarm and color the network element as green once 5620 SAM detects SNMP connectivity to the network is re-established. Details of the alarm are the following:

- Severity: Major
- Type: communicationsAlarm
- Name: SnmpReachabilityProblem
- Cause: SnmpReachabilityTestFailed

This behavior occurs by default and is not configurable.

5.4 SNMP traps

5620 SAM listens to SNMP traps to receive changes from the network elements. 5620 SAM configures the trap log ID on each network element when it is first discovered. The network element then uses that trap log ID to send all configuration changes and updates to 5620 SAM. 5620 SAM will react to the traps it receives and make appropriate changes to the database, alarms and related object as required.

5.5 SNMP trap sequence verification

5620 SAM retrieves the last trap sequence number sent from all network elements at a configurable interval. This interval is configurable on a per resource group basis. Resource groups allow the user to configure the communications behavior of a group of network elements. By default, the core resource group includes all network elements, and verifies the trap sequence number every 4 minutes. 5620 SAM compares that sequence number with the sequence number of the last trap it received from that network element. If they do not match, 5620 SAM will request only the missing traps from the network element. If at any point 5620 SAM realizes that it is missing more than 200 traps from a network element, or if the network element no longer has the missed trap, SAM will request a full resynchronization on that network element rather than just request the missing traps. The SNMP trap sequence verification was added in 5620 SAM Release 3.0

This behavior occurs by default and is not configurable.

5.6 Scheduled SNMP MIB polling

5620 SAM can poll all data SNMP MIBs from the network elements at a configurable interval. Starting in 5620 SAM Release 7.0 R1, the Poller policy is disabled by default. This behavior is configurable via the *Poller Policies* Manager.

5.7 Network outages

When an Alcatel-Lucent 7x50-based network element loses visibility of the 5620 SAM Network Manager, it is unable to send traps to the network manager, and the traps are queued on the network element. Section 5.5 describes 5620 SAM behavior with regards to trap handling. When a network outage occurs, the network element configuration in 5620 SAM will be made consistent with the network element, but any event notifications, such as SNMP traps, that occurred during the network outage will not have been processed. This will cause intermediate state change alarms to not be reflected in 5620 SAM during the network outage.

6 — Network requirements

- 6.1 Network requirements 6-2**
- 6.2 Connectivity to the network elements 6-2**
- 6.3 Bandwidth requirements for collocated 5620 SAM installations 6-2**
- 6.4 Bandwidth requirements for distributed 5620 SAM installations 6-3**
- 6.5 Bandwidth requirements for 5620 SAM GUI Clients 6-6**
- 6.6 Bandwidth requirements for displaying 5620 SAM GUI Clients on X displays 6-7**
- 6.7 Bandwidth requirements for 5620 SAM-O OSS Clients 6-7**
- 6.8 Bandwidth requirements for the 5620 SAM Auxiliary Statistics Collector workstation 6-8**
- 6.9 Bandwidth requirements for the 5620 SAM Auxiliary Call Trace Collector workstation 6-8**
- 6.10 Network latency considerations 6-11**
- 6.11 Network reliability considerations 6-14**
- 6.12 GNE, Alcatel-Lucent OmniSwitch, 7250 SAS, Telco T5C, 9471 MME, eNodeB, and 5780 DSC considerations 6-15**

6.1 Network requirements

The network interconnecting the 5620 SAM systems, network elements, and OSS systems is of significant importance to the effective management of the network. The following sections describe the requirements for the network links between 5620 SAM workstations and the connection to the network being managed. Alcatel-Lucent recommends that sufficient bandwidth be made available to the 5620 SAM workstations within the Data Communication Network.

For SNMP management of Alcatel-Lucent network elements, all network segments that carry SAM management traffic must allow the successful transmission of 9216 byte SNMP packets. The *5620 SAM Troubleshooting Guide* contains more information on packet fragmentation issues.

Be sure to include the tables with the bandwidth required for statistics collection in the total bandwidth required between the 5620 SAM workstations, as they are in separate tables.

The tables do not specify the underlying infrastructure required to support these bandwidth requirements.

See chapter 9 for information on configuring the 5620 SAM workstations with multiple interfaces.

6.2 Connectivity to the network elements

5620 SAM Release 9.0 supports both IPv4 and IPv6 connectivity to network elements. The following network elements may be managed by 5620 SAM using IPv6:

- 7750 6.1, 7.0, 8.0 and 9.0
- 7450 7.0, 8.0 and 9.0
- 7710 6.1, 7.0, 8.0 and 9.0
- eNodeB LA 2.0, LA 3.0, and LA 4.0

6.3 Bandwidth requirements for collocated 5620 SAM installations

Table 6-1 lists the bandwidth requirements for the connections between the components of a 5620 SAM Collocated installation. It is a good practice to measure the bandwidth utilization between the various components to determine a suitable bandwidth. There are a number of factors that could require an increase above our bandwidth utilization recommendations – including: GUI activity, OSS activity, network events, number of network elements being managed.

Table 6-1 5620 SAM collocated Server/Database bandwidth requirements

Available bandwidth required from primary 5620 SAM Server/Database workstation	Recommended bandwidth: excluding statistics and call trace bandwidth requirements
5620 SAM Client (GUI)	512 kbps
5620 SAM-O Client (The bandwidth will depend on the OSS application)	1 Mbps
Between primary and standby 5620 SAM Server/Database workstation NOTE: When network element database backup synchronization is enabled, the bandwidth requirement between the 5620 SAM Servers will vary significantly depending on the size of the network element backup file sizes.	5-10 Mbps (sustained) 16-26 Mbps (during re-instantiation or database backup synchronization)

6.4 Bandwidth requirements for distributed 5620 SAM installations

The following tables list the requirements for the connections between the components of a 5620 SAM Distributed installation. It is a good practice to measure the bandwidth utilization between the various components to determine a suitable bandwidth. There are a number of factors that could require an increase above our bandwidth utilization recommendations – including: GUI activity, OSS activity, network events, number of network elements being managed.

Table 6-2 5620 SAM distributed Server/Database bandwidth requirements

Available bandwidth requirements for 5620 SAM	Recommended bandwidth: excluding statistics and call trace bandwidth requirements
5620 SAM Server to a 5620 SAM Database NOTE: This depends on GUI changes and lists, # of changes occurring in the network, and network objects managed.	5 to 10 Mbps (3 Mbps minimum)
5620 SAM Server to a 5620 SAM Client	512 Kbps
5620 SAM Server to a 5620 SAM-O Client (The bandwidth will depend on the OSS application)	1 Mbps
Between a primary and a standby 5620 SAM Server NOTE: When network element database backup synchronization is enabled, the bandwidth requirement between the 5620 SAM Servers will vary significantly depending on the size of the network element backup file sizes.	1 Mbps
5620 SAM Server to a 5620 SAM Auxiliary Statistics Collector	1 Mbps
Between primary and standby 5620 SAM Databases NOTE: The higher bandwidth is required to handle re-instantiation and is also required immediately after a database backup when database backup synchronization is enabled.	6 Mbps (sustained) 15-25 Mbps (during re-instantiation or database backup synchronization) 3 Mbps (minimum)

The size of the network and the number of statistics that are collected will impact the recommended bandwidth between the following workstations:

- 5620 SAM Auxiliary Statistics Collector and 5620 SAM Database
- Active and Inactive 5620 SAM Database workstations

The following tables should be used to determine how much additional bandwidth will be required between the 5620 SAM workstations when statistics collection is added to the system. The bandwidths of connections not listed do not change dramatically with the addition of statistics.

The registerLogToFile method of retrieving statistics can be compressed or uncompressed. Using the compressed option will require additional CPU requirements on the workstation that is collecting the statistics (either 5620 SAM Server or 5620 SAM Auxiliary Statistics Collector). In this case, the bandwidth required will be reduced.

Table 6-3 Additional bandwidth requirements for accounting statistics collection.

Bandwidth requirements for installations collecting accounting statistics.	Additional bandwidth per 200,000 accounting statistics records
5620 SAM Server to a 5620 SAM-O-O Client if using findToFile. OR 5620 SAM Server to 5620 SAM-O Client if using an uncompressed registerLogToFile (5620 SAM Auxiliary Statistics Collector is NOT installed). OR 5620 SAM Auxiliary Statistics Collector to 5620 SAM-O Client if using an uncompressed registerLogToFile.	3.5 Mbps
5620 SAM Server to 5620 SAM Database workstation if the 5620 SAM Server is collecting the statistics OR 5620 SAM Auxiliary Statistics Collector to 5620 SAM Database workstation if the 5620 SAM Auxiliary Statistics Collector is collecting the statistics	2.2 Mbps
Between the 5620 SAM Database workstations NOTE: The higher bandwidth is required to handle re-instantiation during statistics collection	3.2 Mbps (sustained) 18 Mbps (during re-instantiation or database backup synchronization)

Table 6-4 Additional bandwidth requirements for performance statistics collection.

Bandwidth requirements for installations collecting performance statistics.	Increased Bandwidth per 200,000 performance statistics records
5620 SAM Server to a 5620 SAM-O Client if using findToFile NOTE: a higher bandwidth may be desirable	3.5 Mbps
5620 SAM Server to 5620 SAM Database workstation SUM the following bandwidths: If the 5620 SAM Server is collecting the statistics:(5620 SAM Auxiliary Statistics Collector is NOT installed) If the 5620 SAM-O Client is using findToFile to collect all statistics data	5.4 Mbps 5.4 Mbps
5620 SAM Auxiliary Statistics Collector to 5620 SAM Database workstation if the 5620 SAM Auxiliary Statistics Collector is collecting the statistics	5.4 Mbps
Between the 5620 SAM Database workstations - required for sufficient bandwidth for database re-instantiations NOTE: The higher bandwidth is required to handle re-instantiation during statistics collection	14.4 Mbps (sustained) 72 Mbps (during re-instantiation or database backup synchronization)

Table 6-5 Additional bandwidth requirements for performance management statistics collection.

Bandwidth requirements for installations collecting performance management statistics.	Increased Bandwidth per 200,000 performance management statistics records
Between a primary and a standby 5620 SAM Server: If the 5620 SAM Server is collecting the statistics:(5620 SAM Auxiliary Statistics Collector is NOT installed)	1.0 Mbps
Between a preferred and a reserved 5620 SAM Auxiliary Statistics Collector if the 5620 SAM Auxiliary Statistics Collector is collecting the statistics	1.0 Mbps

Table 6-6 Additional bandwidth requirements for file accounting STM results collection logToFile method.

Bandwidth requirements for installations collecting file accounting STM results using the logToFile method only	Increased Bandwidth per 50,000 file accounting STM records
5620 SAM Server to a 5620 SAM-O Client if using logToFile NOTE: a higher bandwidth may be desirable	3.5 Mbps

When a 5620 SAM Auxiliary Statistics Collector is installed, the bandwidth requirements between two geographic locations will need to reflect the state where a 5620 SAM Auxiliary Statistics Collector in geographic location A may send information to the active 5620 SAM Server in geographic location B which will - in turn – send information back to the 5620 SAM Database in geographic location A. For this reason, the bandwidth between geographic location A and B must be the sum of the bandwidth requirements between the 5620 SAM Auxiliary Statistics Collector to 5620 SAM Server and 5620 SAM Server to 5620 SAM Database. It is also a best practice to ensure that the 5620 SAM Auxiliary Statistics Collector, 5620 SAM Server, and 5620 SAM Database are all collocated in the same geographic site.

5620 SAM Auxiliary Call Trace Collectors

When a 5620 SAM Auxiliary Call Trace Collector is installed, there are a number of bandwidth requirements listed below. Any bandwidths not listed are not impacted significantly by call trace data collection.

To handle the redundant pairs appropriately, the bandwidth requirements between two geographic locations will need to reflect the state where a 5620 SAM Auxiliary Call Trace Collector in geographic location A may need to provide information to the 5620 SAM-O Client in geographic location B. The synchronization of call trace and debug trace files will be impacted by the number client application ftp sessions retrieving call trace and debug trace files. To minimize this impact, it is recommended to limit the number of ftp sessions.

Due to the potential high bandwidth requirements of Call Trace and Debug Trace data, it is recommended to use multiple network interfaces on the Auxiliary Call Trace server. See section 9.4 for recommendations when using multiple network interfaces on an Auxiliary Call Trace server.

Table 6-7 Additional bandwidth requirements for call trace collection.

Bandwidth requirements for installations with call trace collection	Bandwidth usage characterization
5620 SAM Server to a 5620 SAM-O Client	Low bandwidth OSS requests and responses
5620 SAM-O Client to 5620 SAM Auxiliary Call Trace Collector workstation NOTE: a higher bandwidth may be desirable	Higher bandwidth to retrieve via FTP the call trace files from the 5620 SAM Auxiliary
5620 SAM Auxiliary Call Trace Collector Preferred workstation to it's Reserved redundant pair. NOTE: a higher bandwidth may be desirable	Higher bandwidth to ensure timely synchronization of call trace files

6.5 Bandwidth requirements for 5620 SAM GUI Clients

The bandwidth specifications provided above for 5620 SAM GUI Clients are based on the fact that information about changes in the network is forwarded to the 5620 SAM GUI Clients. The 5620 SAM Client updates information visible to the user based on recent changes in the network.

A few examples of network changes which will be reported to 5620 SAM include status changes of physical equipment, status changes of Layer 2 or Layer 3 interfaces, configuration of network elements, provisioning of new equipment or services, status changes in services or any attributes thereof, configuration changes of routing protocols and several others.

In situations where the frequency of changes sent to the 5620 SAM GUI is significant and exceeds the bandwidth specification, the performance of the 5620 SAM Client will degrade, and there is a possibility that the connection to the server will be dropped. A 5620 SAM GUI restart will be required to reconnect to the server to receive change notifications.

6.6 Bandwidth requirements for displaying 5620 SAM GUI Clients on X displays

5620 SAM GUI Clients can be displayed remotely on terminals using the X11 protocol for graphical displays. In these cases, it is important to ensure the bandwidth availability between the workstation running the 5620 SAM Client and the host displaying the 5620 SAM Client be at least 512 Kbps. Also, it is important to ensure the roundtrip network latency between these two hosts is quite low (20-30ms). To achieve acceptable performance on bandwidth limited links, X-compression should be used by using the `ssh -XC` command. If not using compression, it is recommended that the minimum bandwidth be 1024Kbps. Situations where the available bandwidth is lower or the network latency is higher will result in poor usability of the 5620 SAM GUI Client.

Extra bandwidth may be required to support the network elements described in section [6.12](#).

Note that 5620 SAM GUI Client startup may be impacted when using minimum bandwidth links.

6.7 Bandwidth requirements for 5620 SAM-O OSS Clients

There are two main factors affecting the bandwidth requirements between the 5620 SAM Server and a 5620 SAM-O OSS Client:

- Design and behavior of the application using the 5620 SAM-O OSS
- Rate of changes in the network

Applications which listen to network changes via the JMS interface provided by 5620 SAM-O or applications which retrieve large pieces of information via 5620 SAM-O, such as statistics information or network inventory information, will require access to dedicated bandwidth from the machine hosting the application to the 5620 SAM Server according to the tables above. Applications which do not require real time event and alarm notification may operate with acceptable performance when the bandwidth between the machine hosting the application and the 5620 SAM Server is less than the quantity specified in the tables above.

It is a best practice to minimize event and alarm notifications using a JMS filter to reduce bandwidth requirements and the possible effects of network latency.

In an environment where network changes are infrequent, it is possible to successfully operate an application using the 5620 SAM-O when the bandwidth between the machine hosting this application and the 5620 SAM Server is less than the quantity specified in the tables above, possibly as little as 128 kbps. However, in situations where the frequency of network changes increases, the performance or responsiveness of the application will degrade.

6.8 Bandwidth requirements for the 5620 SAM Auxiliary Statistics Collector workstation

The main factors impacting communication to and from the 5620 SAM Auxiliary Statistics Collector workstation are:

- Number of performance statistics being collected. The 5620 SAM Server needs to tell the 5620 SAM Auxiliary Statistics Collector which statistics to collect every interval.
- Number of performance and accounting statistics collected from the network elements.
- Number of performance and accounting statistics written to the 5620 SAM Database.

The more performance statistics are collected, the more significant the bandwidth utilization between the 5620 SAM Server and the 5620 SAM Auxiliary Statistics Collector. Similarly, this will require more significant bandwidth utilization between the 5620 SAM Auxiliary Statistics Collector and the 5620 SAM Database workstations. The bandwidth requirements are not dependent on network activity.

6.9 Bandwidth requirements for the 5620 SAM Auxiliary Call Trace Collector workstation

In order to effectively manage the network, 5620 SAM must have access to sufficient bandwidth between the 5620 SAM Server(s), 5620 SAM Auxiliary(s) and the network elements.

This bandwidth will be used to carry the management traffic between 5620 SAM and the network element. Table 6-8 describes the bandwidth requirements for a particular network element.

Table 6-8 5620 SAM Server to network bandwidth requirements

Number of MDAs/CMAs	Network element Example	Bandwidth requirement from 5620 SAM Server(s) to the network element
2	7450 ESS-1 Telco T5C 7250 SAS	200 kbps
N/A	OmniSwitch 6400, 6850, 6855, 9000 Series	600 kbps
N/A	9500 MPR	200 kbps
10	7450 ESS-7 (fully loaded)	1 Mbps
8	7705 SAR (fully loaded)	200 kbps - 400 kbps
20	7750 SR-12 (fully loaded)	2 Mbps
12	7710 SR C-12(fully loaded)	600 kbps
1	7210 SAS-E	200-300 kbps

(1 of 2)

Number of MDAs/CMAs	Network element Example	Bandwidth requirement from 5620 SAM Server(s) to the network element
N/A	9471 MME	200 kbps
N/A	5780 DSC	200 kbps
N/A	eNodeB (3 Cell)	600 kbps ⁽¹⁾

(2 of 2)

Note

⁽¹⁾ Figure does not include bandwidth required for trace (call and debug) collection.

Details on the bandwidth requirements

The recommended bandwidth described above is a conservative figure that is meant to ensure that the performance of 5620 SAM and its ability to manage successfully each network element will not be affected by unusual network conditions.

Specifically, the bandwidth recommendation ensures that 5620 SAM can fully discover (or resynchronize) all of the objects contained in the network element, within a reasonable amount of time, usually no more than a few minutes for a densely populated network element.

The following are the main operations that result in significant amounts of information being exchanged between 5620 SAM and the network elements. These factors are therefore the principal contributors to the bandwidth requirements.

- **Network Element Discovery:** Upon first discovery of the network element, a significant amount of data is exchanged between 5620 SAM and the network element.
- **SNMP traps:** SNMP traps do not result directly in significant data being sent from the network element to the 5620 SAM. Several of the SNMP traps however do not contain all of the information required for 5620 SAM to completely represent the new status of the network element. As a result, 5620 SAM will subsequently perform a poll of a certain number of the SNMP MIBs to obtain the required information from the network element. Consequently, SNMP traps do result in a certain quantity of data and therefore cause bandwidth utilization. The exact quantity of bandwidth utilized will vary based on the number and the type of trap that is sent from the network element. In the worst case however, this bandwidth utilization will be less than that utilized during a network element discovery.
- **SNMP polling:** It is possible to configure 5620 SAM to poll the SNMP MIBs on the network elements at various intervals. By default, 5620 SAM will perform a complete poll of the SNMP MIBs every 24 hours on non-SR-OS based network elements. During the polling cycle, the amount of data transferred between 5620 SAM and the network element is equivalent to the amount of data transferred during the network element discovery.
- **Statistics collection:** It is possible to configure 5620 SAM to poll the SNMP MIBs on the network elements that contain performance statistics information. During the polling cycle, the amount of data transferred between 5620 SAM and the network element is less than the amount of data transferred during the network element discovery. With the configuration of a 5620 SAM Auxiliary Statistics Collector, the communication from and to the network elements will be distributed between the 5620 SAM Server and a 5620 SAM Auxiliary Statistics Collector.

- Network element backup: It is possible to configure 5620 SAM to request a backup of the network element at specified interval. During the NE backup cycle, the amount of data transferred between 5620 SAM and the network element is less than half of the amount of data transferred during the network element discovery.
- Provisioning of services and deployment of configuration changes: When network elements are configured or when services are provisioned via the 5620 SAM GUI or via application using the 5620 SAM-O interface, a small quantity of network bandwidth is utilized. The amount of data transferred is significantly less than during the network element discovery.
- Initiation and collection of STM tests and their results: When STM tests are initiated, the 5620 SAM Server sends individual requests per elemental test to the network elements. Once the test is complete, the network elements report back using a trap. The 5620 SAM server then requests the information from the network element, and stores it in the database. This can result in a significant increase in network traffic to the network elements.
- Call Trace Information collection: When Call Trace information is collected from the eNodeB, the 5620 SAM Auxiliary Call Trace Collector initiates a Call Trace collection with the eNodeB. The eNodeB responds with a stream of UDP traffic to the 5620 SAM Auxiliary Call Trace Collector that is interpreted and placed on the local hard disk. A third-party client will collect the information from the 5620 SAM Auxiliary Call Trace Collector.

For some network elements, management of the NE includes methods other than standard MIB/SNMP management – for example web-based tools. These network elements may require additional bandwidth above the bandwidth levels stated in table 6-8.

Possible consequences of insufficient bandwidth

In situations where there is less than the recommended bandwidth between the 5620 SAM and the network element, the following are possible consequences:

- The length of time required to perform a network element discovery will increase
- The length of time required to perform a SNMP poll of the network element will increase
- The length of time required to retrieve statistics from the network element will increase
- The proportion of SNMP traps that will not reach 5620 SAM because of congestion will increase. This is significant since 5620 SAM will detect it has missed traps from the network element and will result in 5620 SAM performing additional SNMP polling to retrieve the missing information. This will result in additional data being transferred, which will increase the bandwidth requirements, possibly exacerbating the situation.

Determining total bandwidth requirements for 5620 SAM-managed networks

The amount of bandwidth required for each of the network elements should be obtained from table 6-8.

The total amount of bandwidth that is required for 5620 SAM to manage the complete network will vary based on the topology of the infrastructure that is used to carry the management traffic. From 5620 SAM's perspective, there must be sufficient bandwidth (as per table 6-8) between itself and each of the network elements that is under management.

In cases where the management traffic is carried over physical point-to-point links between the 5620 SAM Server and 5620 SAM Auxiliary network and each of the network elements, sufficient bandwidth must be reserved on the physical links, as per table 6-8. The 5620 SAM Server complex can simultaneously communicate to several NEs for the following functions:

- NE Discovery, NE Resync, Resyncing for Trap Processing
- NE Backups, NE Software Downloading, and sending configurations to NEs
- Collecting Performance Statistics
- Collecting Accounting Statistics
- Initiating STM Tests on NEs
- Retrieve STM Test Results - also via FTP
- NE Reachability checks and NE trap gap checks
- Enabling Call Trace on eNodeB NEs

Rarely are all of the above performed simultaneously so it is recommended to assume for link aggregation points that SAM can communicate with a minimum of 20-30 NEs simultaneously – this can increase to 60-70 NEs on a 16 CPU core 5620 SAM Server workstation. For Networks of over 1,000 NEs or where a SAM Auxiliary Statistics Collector is being used, that number should be increased by 20-30 NEs. Higher bandwidth maybe required under special cases where above average data is attempted to be transferred between SAM and the network elements. For example, large statistics files, NE backups, or software images.

6.10 Network latency considerations

Network latency can potentially impact the performance of the 5620 SAM workstations. The following are known impacts of latency between the various 5620 SAM workstations:

- 5620 SAM Server to 5620 SAM Clients (GUI/OSS): event notification rates of network changes
- 5620 SAM Auxiliary Statistics Collector to the network elements: ftp connection for statistics collection and SNMP stats collection
- 5620 SAM Auxiliary Call Trace Collector to the eNodeB network elements: UDP call trace information received from the eNodeB
- 5620 SAM Server to the network elements: resync times, provisioning, ftp connections for statistics and network element backups, trap handling, and SNMP stats collection (See section 7.3 for more information on latency impact on SNMP stats collection)
- 5620 SAM Server and 5620 SAM Auxiliary to 5620 SAM Database: 5620 SAM performance is sensitive to latency in this area. The roundtrip latency between the active 5620 SAM components (Server, Database, Auxiliary) must be no longer than 1 ms., otherwise overall 5620 SAM performance will be significantly impacted.

Since SNMP communication to a single Network Element is synchronous, the impact of latency is directly related to the number of SNMP gets and responses. Operations to a Network Element with a round trip latency of 50 ms will have the network transmission time increase by ten times compared to a Network Element with a round trip latency of only 5 ms. For example, is a specific operation required 5620 SAM to send 1,000 SNMP gets to a single Network Element, 5620 SAM will spend a total of 5 seconds sending and receiving packets when the round trip latency to the network element is 5 ms. The time that 5620 SAM spends sending and receiving the same packets would increase to 50 seconds if the round trip latency were increased to 50 ms.

Network Element re-sync can be especially sensitive to latency as the number of packets exchanged can number in the hundreds of thousands. For example, if a re-sync consists of the exchange of 100,000 packets (50,000 gets and 50,000 replies), 50 ms of round trip latency would add almost 42 minutes to the overall re-sync time and 100 ms of round trip latency would add almost 84 minutes to the overall re-sync time.

Common geographical location of 5620 SAM workstations

It is ideal to ensure that all 5620 SAM workstations and the 5620 SAM OSS clients are collocated within a geographical site on a high availability network to avoid the impact of network latency.

In cases where geographic redundancy is configured, all active 5620 SAM workstations (server, auxiliary, and database) should be located within a geographical site on a high availability network to avoid the impact of network latency. When a 5620 SAM workstation (server, auxiliary, or database) switchover or failover occurs, a manual intervention may be required to align the workstations on the same geographical site to minimize the performance impact of network latency. This task can be automated by enabling the DB Alignment feature within 5620 SAM.

Optimizing throughput between 5620 SAM workstations

In high-speed, high-latency networks the TCP socket buffer size controls the maximum network throughput that can be achieved. If the TCP socket buffer is too small it will limit the network throughput, despite the fact that the available bandwidth might support much higher transfer rates.

Adjusting the TCP socket buffer size to achieve optimal network throughput may be necessary if the network bandwidth is more than 10mbps and roundtrip latency is higher than 25msec.

The optimal TCP socket buffer size is the bandwidth delay product (BDP). The bandwidth delay product is a combination of the network bandwidth and the latency, or round-trip time (RTT); basically, it is the maximum amount of data that can be in transit on the network at any given time.

For example, given a 20Mbps network with a RTT of 40ms the optimal TCP socket buffer size would be computed as follows:

$$\begin{aligned} \text{BDP} &= 20 \text{ Mbps} * 40\text{ms} \\ &= 20,000,000 \text{ bps} * .04\text{s} \\ &= 800,000 \text{ bits} / 8 \end{aligned}$$


```
= 100,000 bytes  
  
socket buffer size = BDP  
  
= 100,000 bytes
```

In Solaris 10, the default TCP socket buffer size is 49,152 bytes and Alcatel-Lucent supports a maximum value of 500,000 bytes. The buffer size can be modified at the operating system level by changing the value of the *tcp_recv_hiwat* and *tcp_xmit_hiwat* system parameters. To make this change persistent across system reboots, the commands must be added to a system startup script; this can be achieved by executing the following commands as the root user:

```
# cd /etc/init.d  
  
# cat <<"EOF" > increase_tcp_buffer  
  
> #!/sbin/sh  
  
> #  
  
> # Tune the TCP buffer size to improve network throughput  
  
>  
  
> case "$1" in  
  
> start)  
  
> /usr/sbin/ndd -set /dev/tcp tcp_xmit_hiwat 100000  
> /usr/sbin/ndd -set /dev/tcp tcp_recv_hiwat 100000  
  
> ;;  
  
> stop)  
  
> ;;  
  
> *)  
  
> echo "Usage: $0 { start | stop }"  
  
> exit 1  
  
> ;;  
  
> esac  
  
> exit 0  
  
> EOF  
  
# chmod 0744 increase_tcp_buffer
```

```
# chown root:sys increase_tcp_buffer

# ln increase_tcp_buffer /etc/rc1.d/K70increase_tcp_buffer

# ln increase_tcp_buffer /etc/rc2.d/S70increase_tcp_buffer
```

It is important to note that increasing the TCP socket buffer size directly affects the amount of system memory consumed by each socket. When tuning the TCP socket buffer size at the operating system level, it is imperative to ensure the current amount of system memory can support the expected number of network connections with the new buffer size.

Additional 5620 SAM Database throughput optimizations

In addition to the optimizations above, the 5620 SAM Database workstation requires changes to the `sqlnet.ora` and `listener.ora` files that are contained in the `oracle/network/admin` directory. The lines with the `SEND_BUF_SIZE` and `RECV_BUF_SIZE` should be uncommented (delete the “#” character), and set to 3 times the BDP value calculated above. The database should be shutdown when this change is made.

6.11 Network reliability considerations

This section describes network reliability considerations.

Reliability between 5620 SAM components

The 5620 SAM requires reliable network communications between all the SAM Components:

- 5620 SAM Servers
- 5620 SAM Databases
- 5620 SAM Auxiliaries
- 5620 SAM GUI Clients and 5620 SAM Delegate GUI server
- 5620 SAM OSS Clients

The performance and operation of 5620 SAM can be significantly impacted if there is any measurable packet loss between the 5620 SAM workstations. Significant packet loss can cause 5620 SAM reliability issues.

Alcatel-Lucent supports the deployment of 5620 SAM using the Oracle Solaris IP multipathing (IPMP) feature. The support for IPMP is intended only to provide network interface redundancy configured in active-standby mode.

Probe-based IPMP fault detection and load spreading capability of IPMP are not supported.

Please refer to Oracle Solaris 10 documentation on how to configure IPMP.

5620 SAM Server to NE network reliability

The 5620 SAM Server requires reliable network connectivity between the 5620 SAM Server/Auxiliary to the managed network elements. The mediation layer in 5620 SAM is designed to recover from lost packets between the 5620 SAM Server and the network elements; however, these mechanisms come with a cost to performance. Any measurable packet loss will degrade performance of 5620 SAM's ability to manage the Network Elements. The loss of packets between SAM and NE will have an impact on (but not limited to):

- Any SNMP operations to the network elements:
- SNMP Trap processing performance
- Provisioning performance
- Provisioning failures
- Performance statistics collection (possibly to the point where statistics collection will be incomplete)
- STM test operation (initiating test and collecting results retrieval)
- NE discovery and resync performance
- NE discovery and resync failures
- scheduled polling for reachability checks
- Accounting Statistics retrieval (possibly to the point where statistics collection will be incomplete)
- CLI session operation
- NE backup retrieval and software download performance

The following example will highlight the significant impact of lost packets. It only considers the SNMP communication times with one network element. With the default mediation policy configured with an SNMP retry time-out of 10 seconds, and an average round trip latency of 50 ms between 5620 SAM Server and the network element, 5620 SAM will spend a total of 25 seconds sending and receiving 1000 packets (500 SNMP gets and 500 SNMP responses). With a 0.1 % packet loss (1 packet out of the 1,000) the 5620 SAM Server will wait for the retry time-out (10 seconds) to expire before retransmitting. This will cause the time to complete the 500 SNMP gets to increase by 10 seconds – for a total of 35 seconds of communication time, or an increase of 40% over the time with no packet loss. With 0.5 % packet loss, the 500 SNMP gets would increase by 50 seconds – for a total of 75 seconds to complete or an increase of 200%.

6.12 GNE, Alcatel-Lucent OmniSwitch, 7250 SAS, Telco T5C, 9471 MME, eNodeB, and 5780 DSC considerations

5620 SAM Clients support the web-based WebView functionality on OmniSwitch family of switches.

5620 SAM Clients support web-based clients on the GNEs, 7250 SAS, and Telco T5C network elements.

The 5780 DSC and 9471 MME are treated as network elements within 5620 SAM.

The 5780 DSC is managed via a web interface that is run through the browser that is installed on the 5620 SAM Client workstation or 5620 SAM Delegate workstation. It requires a direct connection from the 5620 SAM Client to the 5780 DSC. As such, unique firewall rules are required. There are also increased memory requirements on the 5620 SAM Client and/or 5620 SAM Delegate workstations for the Web Browser.

The 9471 MME requires two management tools to be configured: the MME MI tool, and the Client. Their management includes communication directly from the 5620 SAM Client to the 9471 MME platforms.

The eNodeB NEM is installed along with the 5620 SAM Client and communicates with the eNodeB elements in the network through a UDP proxy configured on the 5620 SAM Server. NEM runs within a separate JVM requiring additional memory resources on the 5620 SAM Client workstation. Please consult the NEM User Guide for up-to-date memory requirements for NEM.

9500 MPR support includes the use of NEtO for specific management functions for these Network Element types. NEtO is a separate application that is installed along with the 5620 SAM Client and launched through the 5620 SAM Client UI. Please consult the 9500 MPR Documentation Suite for current memory requirements that are in addition to the 5620 SAM Client memory requirements.

7 – *Scaling*

- 7.1 Scaling guidelines 7-2**
- 7.2 Scaling guidelines for 5620 SAM OSS Clients 7-3**
- 7.3 Scaling guidelines for statistics collection 7-4**
- 7.4 Scaling guidelines for scheduled tests (STM) 7-8**
- 7.5 Scaling guidelines for call trace 7-14**

7.1 Scaling guidelines

Table 7-1 represents the scalability limits for Release 9.0. Note that:

- These limits require particular hardware specifications and a specific deployment architecture.
- Scale limits for network elements including GNEs, 7705s, and 7210s assume a maximum sustained trap rate of 40 traps/ second for the entire network.

Chapter 4 contains information on identifying the correct hardware platform for a particular network configuration. To achieve these scale limits, a distributed Solaris configuration is required, and may also require a 5620 SAM Auxiliary Statistics Collector and a storage array for the 5620 SAM database workstation. NAS disk configurations are not supported.

Consult Alcatel-Lucent personnel to ensure you have the correct hardware platform and configuration for your network size.

Table 7-1 5620 SAM Release 9.0 R5 scalability limits

Attribute of managed network	Distributed configuration
Maximum number of managed MDAs	25,000
Maximum number of Network Elements (excluding GNEs)	18,000
Maximum number of GNEs ⁽¹⁾	18,000
Maximum number of Network Elements	21,000
Maximum number of managed services	2,000,000
Maximum number of SAPs	6,000,000
Maximum number of simultaneous 5620 SAM GUI	150
Maximum number of simultaneous active 5620 SAM-O HTTP applications	30
Maximum number of simultaneous active 5620 SAM-O JMS applications	10
Maximum number of outstanding alarms	50,000
Maximum number of Alarms (equivalent to 1 month retention assuming 50,000 per day)	2,000,000

Note

- ⁽¹⁾ The number of interfaces on a GNE and the traps that may arise from them is the key factor determining the number of GNE devices that can be managed. As GNE devices are expected to be access devices the sizing is based on an average of 10 interfaces of interest on each device (10 x 18,000 = 180,000 interfaces). Processing of traps from interface types that are not of interest can be turned off in 5620 SAM. Under high trap load, 5620 SAM may drop traps

5620 SAM Release 9.0 uses the number of MDAs as the fundamental unit of network dimensioning. To determine the current or eventual size of a network, the number of deployed or expected MDAs, as opposed to the capacity of each router, must be calculated.

Table 7-2 Network element maximums and equivalency

Network element Type	Maximum number of network elements supported	MDA equivalency
7250 SAS (or Telco T5C CLE)	2,500	5,000
7705	12,000	12,000
7210	12,000	12,000
OMNISwitch 6000 series (each shelf in the stackable chassis)	12,000	12,000
OMNISwitch 9000 series (each NI)	1,000	1,000
9500 MPR	12,000	12,000
eNodeB	8,000	16,000

The 5780 DSC and the 9471 MME have an MDA equivalency of 1 MDA per blade.

The IMM card has an MDA equivalency of 2 MDAs per card.

The CMA card has an MDA equivalency of 1 MDA per card.

7.2 Scaling guidelines for 5620 SAM OSS Clients

There can be a maximum of 10 5620 SAM OSS-JMS Clients.

The number of 5620 SAM OSS-HTTP Clients supported by a 5620 SAM Server workstation is 2 times the number of CPU cores with at least 10 and at most 30 clients supported.

The maximum number of concurrent findToFile operations supported is 5.

5620 SAM OSS Clients using JMS

As of 5620 SAM 9.0R5, OSS Clients using JMS durable connections have a maximum message rate comparable to non-durable clients.

Network latency between the 5620 SAM Server and a 5620 SAM OSS Client will reduce the JMS message rate. For durable JMS clients, the *Duplicate OK* method will allow for a higher message rate than the *Auto Acknowledge* method. Refer to the *5620 SAM-O OSS Interface Developer Guide* for more information.

5620 SAM is also able to deliver hundreds of messages per second to a non-durable 5620 SAM OSS client.

Table 7-3 JMS durable messaging rates

JMS messaging	Roundtrip latency from the OSS Client to the 5620 SAM Server		
	0ms	20ms	40ms
Durable connection with Auto-acknowledge	1000	45	22
Durable with Duplicates-OK	1000	400	212

5620 SAM 3GPP OSS Client

5620 SAM 3GPP OSS Clients connect to the 3GPP interface provided on the 5620 SAM Server. The 3GPP Interface uses a CORBA interface. Network latency between the 5620 SAM Server and a 5620 SAM 3GPP OSS Client will reduce the message rate.

Table 7-4 3GPP OSS JMS messaging rates

CORBA messaging	Roundtrip latency from the OSS Client to the 5620 SAM Server		
	0ms	20ms	40ms
3GPP OSS connection	74	68	53

7.3 Scaling guidelines for statistics collection

5620 SAM provides the ability to collect statistics information from the network elements. This section provides guidelines that can be used to determine the extent to which Statistics Collection can be retrieved from the network.

Statistics collection definitions

Performance statistics: These statistics are associated with various network objects such as ports, interfaces, channels and network elements (routers). These statistics are retrieved by 5620 SAM using SNMP polling according to the MIB policies that are configured by the user.

Accounting statistics: These statistics are associated with Services, Subscribers, and Network Interfaces and contain data that can be used for accounting, billing and SLA management purposes. These statistics are collected on the 7x50 and retrieved by 5620 SAM via a file that is transferred via ftp.

Statistics Item: An individual statistics counter, such as RxOctets or TxFrames.

Statistics Record: A collection of statistics items which is retrieved from the router and stored in the 5620 SAM database as an atomic operations. In the various statistics forms on the 5620 SAM GUI Client, a statistics record appears to the user as a single row which contains the collection or retrieval timestamp and a set of individual statistics items. In the case of performance statistics, a statistics record corresponds to a row in the MIB table.

Determining the number of statistics records that will be collected

In 5620 SAM Release 5.0 and above, statistics can be collected and processed by the 5620 SAM Server or by the 5620 SAM Auxiliary Statistics Collector for dedicated statistics handling. The 5620 SAM Auxiliary Statistics Collector provides a dedicated workstation for statistics collection. The following sections should be used to determine the maximum performance and accounting statistics for different hardware setups.

Performance statistics

Refer to the *5620 SAM Statistics Management Guide* to find the steps required to configure 5620 SAM to retrieve and process performance statistics. Note that two steps are required to enable the collection of performance statistics from the network. First, a policy is defined which specifies a set of polling periods for various MIBs. Second, the policy is applied to a number of network elements.

In general, enabling the statistics collection of a MIB will result in one statistics record being collected, at the specified polling period, for each network object to which the MIB applies.

For example, consider a policy is created with only the rtr.L2AccessDhcpRelayCfgStats MIB enabled for collection at 15-minute intervals. That policy is assigned to only two network elements which each contain 500 L2 Access Interfaces. As a result of this action, 5620 SAM will collect 1,000 statistics records from the network every 15 minutes.

The quantity of resources which are allocated to the retrieval and processing of performance statistics does not depend significantly on the number of CPUs available to the 5620 SAM Server software. Table 7-5 shows the maximum number of performance statistics that can be retrieved and processed by the 5620 SAM Server or 5620 SAM Auxiliary Statistics Collector every 15 minutes.

Table 7-5 Maximum number of performance statistics records processed on a 5620 SAM Server

Number of CPU cores on 5620 SAM Server workstations	Maximum number of performance statistics records per 15-minute interval		
	Collocated configuration	Distributed configuration	Distributed configuration with Auxiliary Statistics Collector
4 or greater SPARC	50,000	100,000	500,000
4 or greater x86	50,000	150,000	1,000,000

To compute the number of CPU cores available on the workstation, the following Solaris command can be used:

```
# /usr/bin/kstat -p cpu_info:::core_id | /usr/bin/awk '{print $NF}' |  
/usr/bin/sort -u | /usr/bin/wc -l
```

In situations where the 5620 SAM Server is asked to collect more performance statistics than it can process in the specified polling period, the *PollerDeadlineMissed* alarms will start appearing. These alarms indicate to the user that the polling mechanisms within 5620 SAM cannot retrieve the requested information within the specified polling period. Should this situation arise, the polling period for statistics should be increased or the number of objects that are applied to Statistics Poller Policies should be reduced.

Performance statistics collection and network latency

5620 SAM collection of performance statistics from a single network element may be limited due to the round trip delay caused by network and network element latency. 5620 SAM collects performance statistics records using SNMP. One record is collected at a time to limit the load on the network element. Therefore, round trip latency will directly impact the maximum number of performance statistics records collected. As an example, if the round trip latency is 100ms, and we target a completion time of 75% of the collection interval (to allow for processing variances and other system impacts), the maximum number of performance statistics records that can be collected from one network element in a 15 minute interval would be 6750 records (75% of 900 seconds divided by 100 ms latency).

Accounting statistics

Refer to the *5620 SAM Statistics Management Guide* to find the steps required to configure 5620 SAM to retrieve and process accounting statistics.

The quantity of resources which are allocated to the retrieval and processing of accounting statistics within the 5620 SAM Server are set at the installation time and depend on the number of CPUs available to the 5620 SAM Server software. The number of CPUs available to the 5620 SAM Server depends on the number of CPUs on the workstation and whether the 5620 SAM Database software is collocated with the 5620 SAM Server software on the same workstation.

An accounting statistic record is the statistic for one queue for one SAP. For example, if 2 ingress and 2 egress queues are configured per SAP, the “Combined Ingress/Egress” statistic represents 4 5620 SAM accounting statistic records.

It is recommended that the Accounting Policy Interval and the File Policy Interval be aligned to the same period. Misalignment of the policy periods can cause 5620 SAM resource contention for both performance and accounting statistics processing.

The following tables provide the maximum number of accounting statistics records that can be retrieved and processed by the 5620 SAM Server or 5620 SAM Auxiliary Statistics Collector in various situations.

To reach the peak accounting statistics from the 5620 SAM Auxiliary Statistics Collector workstation, the 5620 SAM Database workstation requires a customized configuration that can be obtained from Alcatel-Lucent personnel.

Table 7-6 Maximum number of accounting statistics records to be processed by a 5620 SAM Server workstation

Number of CPU cores on 5620 SAM Server workstations	Maximum number of accounting statistics records per 15-minute interval		
	Collocated configuration	Distributed configuration	Distributed configuration with Auxiliary Statistics Collector
4	100,000	200,000	800,000
8 or greater	200,000	400,000	10,000,000 (8 CPU core and 16 GB RAM Oracle or HP x86 Auxiliary Statistics Collector platform required)

5620 SAM Database hardware platform requirements

To collect large numbers of statistics, there are RAM and disk drive requirements for the 5620 SAM Database workstation. Table 7-7 highlights these requirements.

Table 7-7 5620 SAM Database workstation hardware requirements for a distributed configuration

Maximum number of simultaneous statistics records per 15-minute interval		5620 SAM Auxiliary Statistics Collector	Requires the following 5620 SAM Database workstation setup
Accounting statistics records	Performance statistics records		
400,000	0	No	4 CPU cores 4 disk 8 GB RAM
0	150,000	No	
800,000	0	Yes	4 CPU cores 4 disk 16 GB RAM
0	200,000	Yes	
10,000,000	500,000	Yes	8 CPU cores Customized disk configuration required ⁽¹⁾ 32 GB RAM
10,000,000	1,000,000	Yes	12 CPU cores Customized disk configuration required ⁽¹⁾ 48 GB RAM

Note

⁽¹⁾ Please contact Alcatel-Lucent for the most current layout, appropriate to your configuration

To compute the number of CPU cores available on the workstation, the following Solaris command can be used:

```
# /usr/bin/kstat -p cpu_info:::core_id | /usr/bin/awk '{print $NF}' |
/usr/bin/sort -u | /usr/bin/wc -l
```

In situations where the 5620 SAM Server is asked to collect more accounting statistics records than it can process in the specified retrieval period, the extra statistics will not be retrieved from the network.

There are two methods to export accounting and performance statistics from 5620 SAM: `registerLogToFile`, and `findToFile`. The `registerLogToFile` method is the preferred method and is required for situations where more than 400,000 accounting statistics records are retrieved in 15 minutes or 500,000 performance statistics are retrieved in 15 minutes. This recommendation also minimizes collection latency and reduces system load.

Simultaneous collection of performance and accounting statistics records

5620 SAM can collect both performance and accounting statistics records simultaneously. However, it is important to consider that enabling the collection of one type of statistics will reduce the capability of 5620 SAM to collect and process the other type of statistics. It is therefore not possible to achieve the maximum stated limits for both performance and accounting statistics records simultaneously. Table 7-7 shows an example of simultaneous collection.

Determining the number of performance and accounting statistics records being collected by 5620 SAM

To ensure the number of performance and accounting statistics records that 5620 SAM is asked to collect and process every 15 minutes remains below the stated scalability guidelines, it is important to carefully assess the impact of creating and assigning statistics policies. Review the number of objects that are assigned to statistics policy and ensure the polling and retrieval periods are set such that the numbers will remain below the stated guidelines.

Using SAM performance statistics, 5620 SAM can assist in determining how many polled and accounting statistics are being collected.

5620 SAM performance can be adversely affected by increasing the number of historical statistics entries recorded by the 5620 SAM. 5620 SAM system impacts include increased time listing log records from the GUI and OSS clients, increased Oracle tablespaces, and increased database backups times.

7.4 Scaling guidelines for scheduled tests (STM)

5620 SAM provides the ability to generate, manage and schedule STM tests within the network. This section provides guidelines that can be used to determine the extent to which STM tests can be scheduled and launched within a network.

There are a number of factors which will influence 5620 SAM's ability to concurrently manage and schedule a large number of tests. 5620 SAM keeps track of how many tests are running concurrently. This is to limit the initiation of the tests, and the processing of the results without interfering with the system's other functions.

To understand the STM guidelines, the following terminology is required:

Elemental Test: An OAM test to be sent to a router such as an LSP ping

Lightweight Test: An OAM test that is initiated in the default manner, however, will no longer record individual test and probe results in SAM unless the test has failed.

Accounting file Test: An OAM test that is initiated in the default manner, however, the test results are retrieved from the network element via FTP on a periodic basis.

Test Policy: A definition or configuration that tells 5620 SAM the specifics about how to generate a test. A test policy can contain multiple test definitions. The policies are used by test suites.

Test Suite: A collection of elemental tests that can be assigned to a specific schedule. There are three defined sections in which tests can be placed within a test suite: First run, Generated and Last run. The tests are executed in order by these sections. It is possible to configure the execution order of tests within the First Run and Last Run sections to be parallel or sequential. The tests in the Generated position are run by the system as concurrently as possible. If the Generated section contains tests from several different test definitions, then all the tests belonging to one definition will be executed before the tests of the next definition begin. Within a definition, the system will attempt to execute the tests as concurrently as possible. This is important to note, as a test suite containing a large number of tests in the Generated section (or in the First Run/Last Run sections set to parallel) may tax the system. Part of the increased stress placed on the system by concurrent tests is a result of the need for the system to use greater amounts of resources in order to initiate, wait for and process many tests concurrently. As well, tests that result in a large amount data to be returned from the routers will place increased demands on the 5620 SAM.

Schedule: A start time that can have a test suite or test suites assigned to it to produce scheduled tasks. When the schedule's start time is reached, the suite or suites assigned to it will commence. The schedule may be set to continuously repeat after a configurable period of time.

Scheduled Task: An instance of a test suite assigned to a schedule

Table 7-8 Maximum number of STM elemental tests

5620 SAM platform	Maximum (regular or lightweight) STM tests in a 10 minute period	Maximum accounting file STM tests in a 10 minute period with results stored in the SAM Database or SAM Database and using logToFile	Maximum accounting file STM tests in a 10 minute period using logToFile only
Distributed Oracle or HP x86 platforms with minimum 8 CPU Core 5620 SAM Server	6,000	50,000	200,000 ⁽¹⁾
Distributed Oracle or HP x86 platform. NOTE: It may be possible to achieve higher numbers depending on the 5620 SAM Server activity and hardware platform	2,000	15,000	40,000
Minimum Collocated Supported Oracle or HP x86 platforms NOTE: It may be possible to achieve higher numbers depending on the 5620 SAM Server activity and hardware platform	1,000	1,000	10,000

(1 of 2)

5620 SAM platform	Maximum (regular or lightweight) STM tests in a 10 minute period	Maximum accounting file STM tests in a 10 minute period with results stored in the SAM Database or SAM Database and using logToFile	Maximum accounting file STM tests in a 10 minute period using logToFile only
Minimum distributed SPARC platform (5620 SAM Server and 5620 SAM database on 4 core v440/v445 Server)	1,000	1,000	1,000
Minimum SPARC platform (collocated 5620 SAM Server and 5620 SAM database on a single 4 core v440/v445 Server)	800	800	800

(2 of 2)

Note

(1) may require a dedicated disk or striped disks for the xml_output partition

Guidelines for maximizing STM test execution:

By default, 5620 SAM will only allow test suites with a combined weight of 80,000 to run concurrently. The test suite weights are identified in the 5620 SAM GUI's Test Suites List window. Running too many tests that start at the same time will cause the system to exceed the previously mentioned limit, and the test will be skipped. Ensuring the successful execution of as many STM tests as possible requires planning the schedules, the contents, and the configuration of the test suites. The following guidelines will assist in maximizing the number of tests that can be executed on your system:

- When configuring Tests or Test Policies, do not configure more packets (probes) than necessary, as they increase the weight of the Test Suite.
- A test suite with a high weight (i.e.: greater than half of the concurrent weight limit) will continue to consume the system's available weight until the test suite has completed executing or until the test suite has timed-out. Test Suite's with a smaller weight will typically complete more quickly, and allow other test suites to execute concurrently. The weight of the test suite is determined by the number of tests in the test suite, and the number of probes that are executed by each test.
- Assign the time-out of the test suite in such a way that if one of the test results has not been received it can be considered missed or failed without stopping other test suites from executing.
- Rather than scheduling a Test Suite to execute all tests on one network element, tests should be executed on multiple network elements to allow for concurrent handling of the tests on the network elements. This will allow the test suite results to be received from the network element and processed by 5620 SAM more quickly freeing up available system weight more quickly.
- Rather than scheduling a test suite to run sequentially, consider duplicating the test suite and running the test suites on alternating schedules. This allows each test suite time to complete or time-out before the same test suite is executed again. Remember that this may cause double the system weight to be consumed until the alternate test suite has completed.
- Test that can be NE persistent should use NE persistence to reduce the interactions between 5620 SAM and the network elements when initiating a test.

- Create test suites that contain less than 200 elemental tests. This way you can initiate the tests at different times by assigning the test suites to different schedules thereby having greater control over how many tests are initiated or in progress at any given time.
- Prioritize which tests you wish to perform by manually executing the test suite to determine how long it will take in your network. Use that duration with some added buffer time to help determine how much time to leave between schedules or repetitions of a schedule and how to configure the test suite time-out.
- A test suite time-out needs to be configured to take effect before the same test suite is scheduled to run again, or it will not execute if it does not complete before the time-out.
- 5620 SAM Database backups can impact the performance of STM tests.
- The Maximum STM Test Results should be configured to be the minimum required number of results. The default is 1,000,000. The maximum is 10,000,000. The more tests that are retained, the slower the 5620 SAM server access to the database will be.
- Attempting to delete tests or test suites manually with large numbers of test results will result in STM test execution delays. The 5620 SAM Server will remove test results as the total number of test results stored exceeds the user configured Maximum STM Test Results. They will age-out.

Lightweight STM test configuration

In 5620 SAM Release 6.0 R3, the concept of lightweight STM test execution was introduced. To take advantage of lightweight test execution, the tests must be NE schedulable with “Lightweight Execution” and “Ignore Probe results” selected. While this can reduce the load on the 5620 SAM Database workstation, it may not increase the maximum number of allowable tests to be executed. Test Suite Results will continue to be produced for each Test Suite execution.

Accounting file STM test configuration

In 5620 SAM Release 7.0 R4, the concept of accounting file collection of STM test results was introduced. This feature requires 7750 and 7450 network elements that are version 7.0 R4 and above. To take advantage of accounting file STM test execution, the test policy must be configured to be NE schedulable with “Accounting file” selected. This will produce STM tests that will be executed on the network element, while the test results will be returned to 5620 SAM by way of an accounting file in a similar way to accounting Statistics.

5620 SAM 9.0R5 supports the use of logToFile for file accounting STM results. When using this method only for results, the number of tests that can be executed per 10 minute interval is increased. Refer to table 7-8 for specific scaling limits. The logToFile method for file accounting STM results supports a maximum of two JMS clients.

Examples of STM test configuration

The following examples describe the configuration of STM tests on different network configurations.

Example 1

Assume there is a network with 400 LSPs and that the objective is to perform LSP pings on each LSP as frequently as possible. The following steps are to be followed:

- 1 Create 4 test suites each containing 100 elemental LSP ping tests
- 2 One at a time, execute each test suite and record the time each one took to complete. Assume that the longest time for executing one of the test suites is 5 minutes.
- 3 Create a schedule that is ongoing and has a frequency of 10 minutes. This doubles the time taken for the longest test suite and ensures that the test will complete before it is executed again. Assign this schedule to the 4 test suites.
- 4 Monitor the test suite results to ensure that they are completing. If the tests are not completing (for example getting marked as “skipped”), then increase the frequency time value of the schedule.
- 5 In the above case, there are 200 elemental tests configured to be executed each 10 minutes.

Example 2

Assume there are eight test suites (T1, T2, T3, T4, T5, T6, T7 and T8), each containing 50 elemental tests. Assume the test suites individually take 5 minutes to run. Also, assume the objective is to schedule them so that the guideline of having less than 200 concurrently running elemental tests is respected.

The recommended approach for scheduling these tests suites is as follows:

- Test suites T1, T2, T3, T4 can be scheduled on the hour and repeat every 10 minutes
- Test suites T5, T6, T7, T8 can be scheduled on the hour + 5 minutes and repeated every 10 minutes

This will ensure no more than 200 elemental tests are scheduled to run concurrently.

Factors impacting the number of elemental tests that can be executed in a given time frame.

The following factors can impact the number of elemental tests that can be executed during a given time frame:

- The type of tests being executed. Each type of elemental test takes varying quantities of time to complete (e.g. a simple LSP ping of an LSP that spans only two routers may take less than 2 seconds; an MTU ping could take many minutes).
- The amount of data that is generated/updated by the test within the network elements. 5620 SAM will have to obtain this information and store it in the 5620 SAM database. The quantity of data depends on the type of tests being performed and the configuration of the objects on which the tests are performed.
- The number of test suites scheduled at or around the same time
- The number of tests in a test suite

- The number of routers over which the tests are being executed. Generally, a large number of tests on a single router can be expected to take longer than the same number of tests distributed over many routers.
- A 5620 SAM Database backup may temporarily reduce the system's ability to write test results into the database.
- The workstation used to perform the tests will dictate how many physical resources 5620 SAM can dedicate to executing elemental tests. On the minimum supported Solaris workstation (collocated 5620 SAM Server and 5620 SAM Database on a single Sun Fire v440/v445 Server), the number of concurrent tests must be limited to 1000.

Possible consequences of exceeding the capacity of the system to perform tests

5620 SAM will exhibit the following symptoms if the number of scheduled tests exceeds the system's capacity.

Skipped tests:

If a test suite is still in progress at the time that its Schedule triggers again, then that scheduled task will be marked as skipped and that test suite will not be attempted again until the next scheduled time.

Failed tests (time-out):

Tests may time-out and get marked as failed. If any of the tests take more than 15 minutes it may get purged from an internal current test list. For example, a test may be successfully sent to a router and the system does not receive any results for 15 minutes. The system marks the test as failed and purges its' expectation of receiving a result. However, later, the system could still receive the results from the router and update its result for the test to success.

Disk space requirements for STM test results:

STM test results are stored in the tablespace DB partition. The STM database partitions start with a total size of 300MB of disk space. When the maximum number of test results is configured at 10,000,000 (maximum), the disk space requirement for the STM tests may increase by up to 40GB. A larger tablespace partition should be considered.

The maximum number of test results stored in the database reflects the sum of the aggregate results, test results, and probe results.

Running 10 tests with 1 probe each versus 1 test with 10 probes consumes the same amount of disk space.

When using logToFile for accounting file STM test results, the maximum time-to-live on the disk is 24 hours. At the maximum collection rate of 200,000 test results per 10 minutes, the storage requirements on the 5620 SAM Server in the xml_output directory is 120GB per JMS client. The storage requirements are doubled if using the maximum number of JMS clients for file accounting STM results. The disk storage requirements can be decreased by using the compress option for logToFile but will result in increased CPU utilization on the SAM Server.

7.5 Scaling guidelines for call trace

5620 SAM provides the ability to collect call trace and debug trace data from eNodeB network elements through the use of 5620 SAM Auxiliary Call Trace Collector workstations.

Call Trace scale support in 5620 SAM is dependent upon the following dimensions:

The network bandwidth required between the 5620 SAM Auxiliary Call Trace server and the eNodeB. This will be determined by the size of the call Trace files and the frequency in which they are collected.

The network bandwidth required between the Preferred 5620 SAM Auxiliary Call Trace server and the Reserved 5620 SAM Auxiliary Call Trace server.

The network bandwidth required between the Preferred 5620 SAM Auxiliary Call Trace server and the 9958 WTA.

Disk I/O on the 5620 SAM Auxiliary Call Trace server.

Disk space on the 5620 SAM Auxiliary Call Trace server to meet the retention requirements.

Call Trace Scaling guidelines are based upon the FDD Outdoor M2 call model which uses a traffic mix of 50% data and 50% voice.

A single 5620 SAM Auxiliary Call Trace Collector workstation or redundant pair can collect up to 50 call traces and two dynamic debug traces concurrently, when deployed in an eight disk configuration. A call trace, in this context, represents the data collected from a single 3 cell eNodeB with 100 calls.

Disk space requirements for Call Trace and Debug Trace

Call Traces and debug Traces retrieved from eNodeBs are stored as files on the 5620 SAM Auxiliary Call Trace Collector. Table 7-9 lists the required disk space to store one hour worth of Call Trace and Debug Trace data from a single 3 cell eNodeB with 100 calls. The disks containing the Call Trace and Debug Trace data must be configured with hardware RAID 0, or disk striping.

Table 7-9 Disk space requirements for trace data.

Disk space requirements for installations with trace collection for a single 3 cell eNodeB with 100 calls for 1 hour of data	Required Disk Space
Call Trace	650 MB ⁽¹⁾
Debug Trace	9200 MB

Note

⁽¹⁾ Worst case as data is compressed and better compression rates may be achieved

8 — Security

- 8.1 Securing 5620 SAM 8-2**
- 8.2 Operating system installation for 5620 SAM workstations 8-2**
- 8.3 5620 SAM software installation 8-3**
- 8.4 5620 SAM network element communication 8-3**
- 8.5 5620 SAM and firewalls 8-3**
- 8.6 Ports required for firewalls 8-5**
- 8.7 FTP between the 5620 SAM Server and 5620 SAM Auxiliary
Statistics Collector and the managed network 8-11**
- 8.8 Firewall and NAT rules 8-12**

8.1 Securing 5620 SAM

Alcatel-Lucent recognizes the importance of deploying important software such as the 5620 SAM in secure environments and, as such, supports the use of security techniques to enhance the security of the 5620 SAM.

5620 SAM communications can be secured using SSL, SNMPv3 and HTTPs. Refer to the *5620 SAM User Guide* for configuration procedures.

Alcatel-Lucent recommends the following steps to achieving 5620 SAM workstation security:

- Install a clean Solaris 10 operating system environment with the minimum required packages documented in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
- Install the latest Solaris Recommended Patch Cluster from Oracle (available at www.oracle.com)
- Enable Solaris Secure by Default feature as described in section 8.2
- Implement firewall rules for the 5620 SAM Servers to control access to ports on 5620 SAM platforms as described in section 8.5
- Installation of 5620 SAM with a secure configuration described in section 8.3
- Network Element connection configuration as described in section 8.4

8.2 Operating system installation for 5620 SAM workstations

Alcatel-Lucent supports customers applying Solaris or Windows patches provided by Oracle or Microsoft which will include security fixes as well as functional fixes. If a patch is found to be incompatible with the 5620 SAM, the patch may need to be removed until a solution to the incompatibility is provided by Oracle, Microsoft, or Alcatel-Lucent. Consult the *Alcatel-Lucent 5620 SAM Release 9.0 Release Notice* documents for up-to-date information about the recommended Solaris maintenance update and patch levels.

5620 SAM is supported on Solaris installed with the list of required Solaris Packages and Ports documented in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Additional efforts to secure the system could impact 5620 SAM's operation or future upgrades of the product. Customer's should perform some level of basic testing to validate additional platform hardening does not impact 5620 SAM's operation. Also, the 5620 SAM Product Group makes no commitment to make 5620 SAM compatible with a customer's hardening requirements.

Required Solaris services

The installation of Solaris 10 leaves many network services enabled by default. To reduce the security risk to a 5620 SAM Server running on Solaris 10, the Solaris "Secure by default" feature can be used to disabled all network services other than SSH. Enabling of this feature is done using the `netservices limited` command. This command should only be executed when the SAM Software is shut down because it will cause some processes to restart.

The only Solaris network services that the 5620 SAM requires are:

- SSH - secure shell
- network time protocol service (ntp) - or some time synchronization service

See Solaris documentation for more information on "Secure by Default".

8.3 5620 SAM software installation

Alcatel-Lucent recommends the following steps when installing the 5620 SAM Servers:

- Configure the 5620 SAM Server IP validation during the 5620 SAM database installation to ensure that only the specified IP address can communicate with the 5620 SAM database. This is documented in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
- Configure SSL for secure communication between the 5620 SAM Server and 5620 SAM Clients (OSS and UI) as documented in the *5620 SAM User Guide*

Alcatel-Lucent recommends the configuration (as documented in the *5620 SAM User Guide*) of the following options to secure communication with the 5620 SAM Client UI and 5620 SAM Client OSS interfaces:

- Password history count
- Password expiry periods
- Client timeouts
- Security statements
- Scope of command and Span of Control
- Client IP validation

8.4 5620 SAM network element communication

The following configurations are documented in the *5620 SAM User Guide*, and help secure communication between the network elements and 5620 SAM server installations:

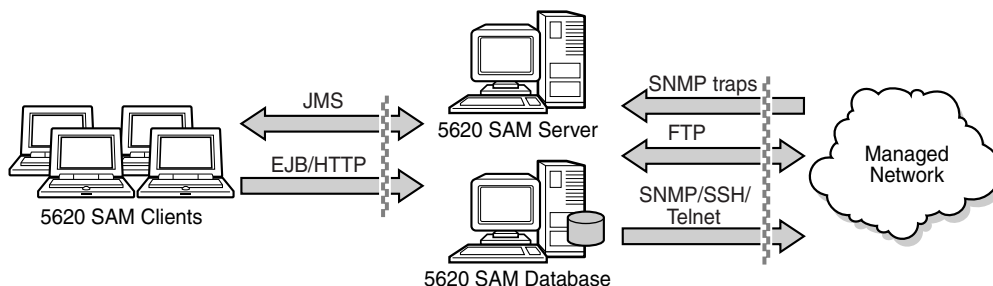
- SNMPv3
- SSH for remote access to the network elements
- SCP/SFTP for secure file transfer

8.5 5620 SAM and firewalls

A firewall can be deployed to protect the 5620 SAM server from the managed network and to protect the server from the network hosting the 5620 SAM clients. The diagrams below illustrate this and show the communications services that are required through the firewalls.

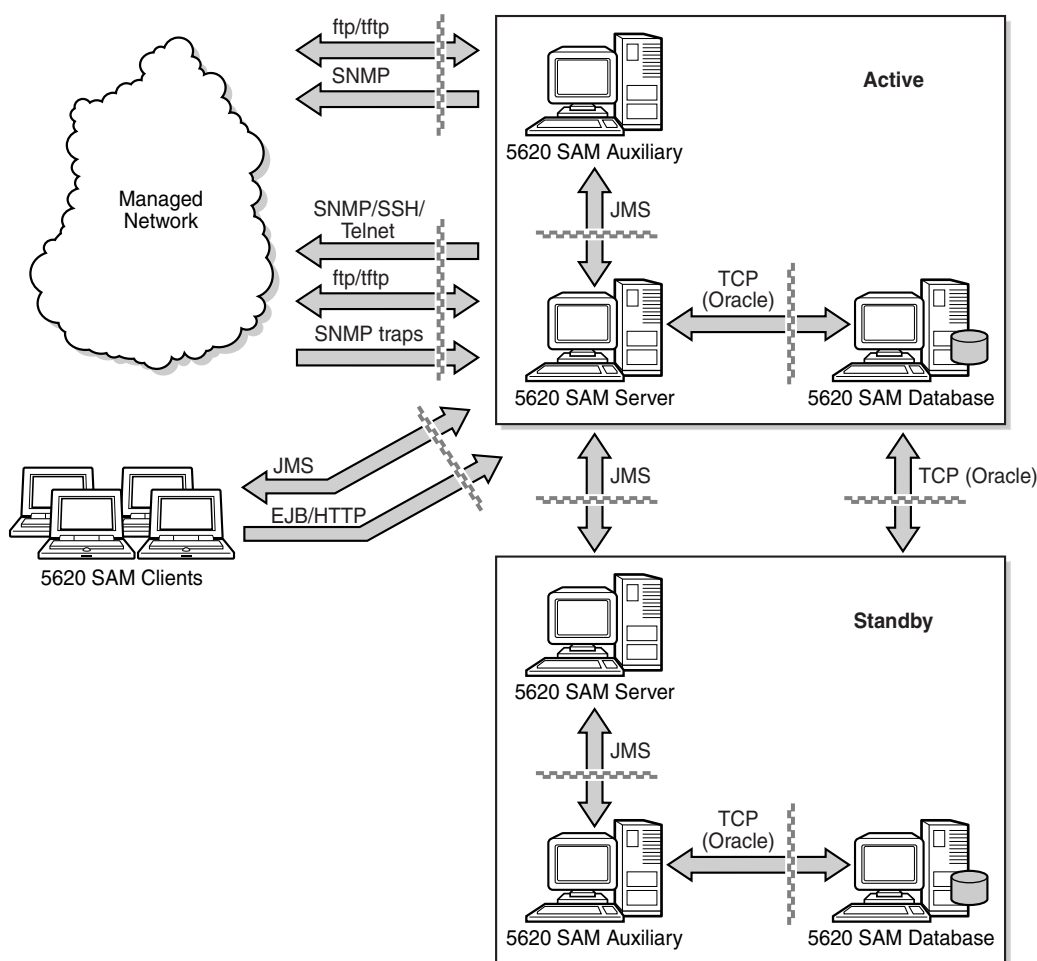
NOTE: For the network elements described in Section 6.12 there is a requirement for the 5620 SAM GUI client to communicate directly with the specialize configuration tools.

Figure 8-1 Firewalls and 5620 SAM standalone deployments



22668

Figure 8-2 Firewalls and 5620 SAM redundant deployments



22667

8.6 Ports required for firewalls

Table 8-1 describes the ports which must be opened in order for the application components to communicate effectively using firewalls.

Table 8-1 5620 SAM firewall requirements

Component	Default port	Type	Encryption	Description
5620 SAM Server and 5620 SAM Auxiliary	N/A	ICMP	N/A	ICMP Ping The active 5620 SAM Server will periodically ping the 5620 SAM Delegate Server to ensure reachability.
	21 Ports from 1023 - 65536	TCP	None. See SCP and SFTP as secure alternatives	FTP (Passive) This port is used to enable ftp communication from a 5620 SAM-O Client to either the 5620 SAM Server or Auxiliary. Ftp is used by the 5620 SAM-O Client to retrieve logToFile statistics or findToFile results. (See section 8.7)
	22	TCP	Dynamic Encryption Cyber Suite and strength as per RFC 4253	SSH/SCP/SFTP This port is used for remote access, rsync between 5620 SAM Servers, rsync between the 5620 SAM Databases, and scp/sftp to 5620 SAM OSS clients.
	69	UDP	None.	TFTP This port is used to do ftp when managing 7250 SAS or Telco T5C equipment. If there are no 7250 SAS or Telco T5C nodes in the network, this port is not required
	162	UDP	Static Encryption When SNMPv3 is configured. Cipher and strength is NE dependant.	SNMP traps By default, this port on the 5620 SAM Server receives SNMP traps from the network elements. This item is specified during the installation of the server and can be changed. (Not required by the 5620 SAM Auxiliary)
	1094, 1095, 4448	TCP	None.	Internal system communications protocol (JBoss messaging) These ports are used by commands on the 5620 SAM Auxiliary workstation to adjust the 5620 SAM Auxiliary behaviour. (Example: adjusting log levels, shutting down the auxiliary server, etc)
	1096, 1097, 4446, 4447	TCP	None.	Internal system communications protocol (JMS naming/messaging service) Used by the 5620 SAM Client (GUI and OSS) and 5620 SAM Server and 5620 SAM Auxiliary applications to register for JMS notifications and messages. This is used to ensure that the Client, Server, and Auxiliary are aware of system events (i.e.: database changes or alarm notifications, etc) NOTE: OSS clients should not use 1097 to access 5620 SAM. They should use 1099 or 1100.
	1098	TCP	None.	Internal system communications protocol (JBoss Naming Service - JNDI) This port is required to ensure successful communication between the 5620 SAM Server and the 5620 SAM GUI and OSS clients. 5620 SAM GUI and OSS clients use this port to look up items provided by the 5620 SAM Server. The items looked up are functions that the clients use to get or send information to and from the server. When there are redundant servers, this port is also used between the two servers to trade information on which items are available for look up.

(1 of 6)

Component	Default port	Type	Encryption	Description
5620 SAM Server and 5620 SAM Auxiliary (continued)	1099	TCP	None.	Internal system communications protocol (JBoss Naming Service -JNDI) This port is required to ensure the 5620 SAM GUI and OSS clients properly initialize with the 5620 SAM Server. When initially logging into the 5620 SAM Server, 5620 SAM GUI and OSS clients use this port to find the various services that are available. This port is also used by the 5620 SAM GUI and OSS clients to register with the 5620 SAM Server to receive notification of network changes.
	1100	TCP	None.	Internal system communications protocol (JBoss High Availability JNDI) This port is required to ensure the 5620 SAM GUI and OSS clients properly initialize with the 5620 SAM Server when there are redundant servers. This port is used when 5620 SAM is installed in a redundant configuration. When initially logging into the 5620 SAM Server, 5620 SAM GUI clients use this port to find the various services that are available. This port is also used by the 5620 SAM GUI and OSS clients to register with the 5620 SAM Server to receive notification of network changes.
	4444, 4450	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported.	Internal system communications protocol (JBoss messaging) During run-time operations, the 5620 SAM GUI clients use this port to send and receive information to and from the 5620 SAM Server. These ports can be encrypted. For example, GUI user operations, such as clicking "apply" on a configuration form, will result in information being transmitted to the server using this port. Note that 5620 SAM can be configured to use a different port for this purpose. The procedure is available from Alcatel-Lucent Personnel.
	4712, 4713, 4812, 4813, 4912, 4913	TCP	None.	Internal system communications protocol used for Transaction processing
	6100-6119	UDP	None.	NEM Proxy Used to provide NEM eNodeB access from SAM Clients.
	8080	TCP	None. See port 8443 for secure communications	HTTP This port provides an HTTP interface for 5620 SAM-O clients to access the 5620 SAM server.
	8085	TCP	None. See port 8444 for secure communications.	HTTP This port provides an HTTP interface for 5620 SAM client. The 5620 SAM Client uses this port to verify the existence of the server.
	8093, 8094	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported	JMS (Java Message Service) This port is used by the 5620 SAM server to send real-time notifications of changes that have happened in the network such as alarms or newly created configurations to the 5620 SAM GUI clients and registered 5620 SAM-O OSS applications. The messages are sent using the JMS protocol (over TCP).
	8400	TCP	None. See port 9400 for secure communications.	HTTP This port provides an HTTP interface for SAM Supervision and the User Documentation Server (InfoCenter).

(2 of 6)

Component	Default port	Type	Encryption	Description
5620 SAM Server and 5620 SAM Auxiliary (continued)	8443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported	HTTPS This port provides an HTTPS (secure HTTP) interface for 5620 SAM-O clients that wish to use this protocol to access the 5620 SAM server
	8444	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported	HTTPS This port provides an HTTPS (secure HTTP) interface for 5620 SAM Client. This is a secure version of port 8085. Used only if 5620 SAM Client is connecting via SSL.
	9010	TCP	None.	This port is used to synchronize: Call Trace and Debug Trace files between redundant Auxiliary Call Trace Collectors, Performance Management statistics between redundant SAM Servers or redundant Auxiliary Statistics Collectors (if present), and snapshots and work orders between redundant SAM Servers.
	9400	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported	HTTPS This port provides an HTTPS (secure HTTP) interface for SAM Supervision. This is a secure version of port 8400. Used only if 5620 SAM Client is connecting via SSL.
	9735	TCP	None.	Corba Interface This port is used by 5620 SAM-O 3GPP-compliant clients to access the 5620 SAM-O 3GPP Corba interface
	11800 Ports from 32768-65536	TCP	Static Encryption Encryption provided by AES Cipher Algorithm with 128 bit Cipher Strength.	Internal system communications protocol (JBoss Clustering) This port is required to ensure that redundant 5620 SAM Servers can monitor each other.
	12300 - 12307	TCP	None.	These ports are used for detecting communication failures between SAM server clusters (Primary / Secondary / Auxiliaries)
	12800	TCP	Static Encryption Encryption provided by AES Cipher Algorithm with 128 bit Cipher Strength.	Internal system communications protocol (JBoss clustering) During run-time operations, the 5620 SAM Auxiliary use this port to send and receive information to and from the 5620 SAM Server. The number of required ports depends on the number of 5620 SAM Auxiliary workstations that are installed. Note that 5620 SAM can be configured to use a different port for this purpose. The procedure is available from Alcatel-Lucent Personnel.

(3 of 6)

Component	Default port	Type	Encryption	Description
Managed Devices	21 Ports from 1023 - 65536	TCP	None.	FTP (Passive) This port is used to enable ftp communication between the 5620 SAM Server and the managed routers. Ftp occurs to transfer information from the routers to the 5620 SAM Server such as accounting statistics. See section 8.7 for a more detailed description of ftp requirements.
	22	TCP	Dynamic Encryption Cyber Suite and strength as per RFC 4253	SSH / SFTP This port used by clients to request a SSH session to a managed router. Used by eNodeBs to transfer software loads from the 5620 SAM Server.
	23	TCP	None.	Telnet This port used by clients to request a telnet session to a managed router.
	80	TCP	None.	HTTP This port is required for the 5620 SAM Client to communicate with the network element Web GUIs. See Section 6.12 for the network elements that require this port.
	161	UDP	Static Encryption When SNMPv3 is configured. Cipher and strength is NE dependant.	SNMP By default, 5620 SAM server sends SNMP messages, such as configuration requests and service deployments, to this port on the network elements.
	443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported	HTTPS This port is required for the 5620 SAM Client to be able to communicate with the 5780 DSC.
	830	TCP	Dynamic Encryption Cyber Suite and strength as per RFC 4253	SSH for eNodeB / SSHv2 for MME This port is used by the eNodeB and MME network elements for NetConf management.
	1099	TCP	None.	RMI This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
	1234	TCP	None.	Search-agent This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.

(4 of 6)

Component	Default port	Type	Encryption	Description
Managed Devices (continued)	1235	TCP	None.	Mosaicsyscv1 This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
	4567	TCP	None.	Tram This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
	5001	TCP	None.	Proprietary Java socket connection This port is used by CPAM to communicate with the 7701 CPAA to obtain control plane information.
	5510	UDP	None.	Trap Trap port used by 9500 MPR devices to send traps to SAM Clients running the NetO manager.
	8001	UDP	Static Encryption When SNMPv3 is configured. Cipher and strength is NE dependant.	SNMP This port is used for SNMP communication with the 9471 MME MI
	8443	TCP	Static Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported	HTTPS This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
	9683	TCP	Static Encryption Encryption provided by SSL/TLS. Both weak and strong ciphers are supported. Full suite of ciphers provided by SSL/TLS are supported	HTTPS This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME Provisioning GUI.
	11500	TCP	None.	Equipment View Used while managing 9500 MRP (MSS-1C, MPR-e) NEs using the Equipment View function as part of NetO
	57074 57075	UDP	None.	Call Trace Data This port is required by the 5620 SAM Auxiliary Call Trace Collector to retrieve the Call Trace information from the eNodeB. Port 57075 is only required by authorized Alcatel-Lucent personnel for debugging purposes.

(5 of 6)

Component	Default port	Type	Encryption	Description
Managed Devices (continued)	N/A	ICMP	N/A	ICMP Only used if the Ping Policy is enabled as part of network element mediation.
5620 SAM Database	22	TCP	Dynamic Encryption Cyber Suite and strength as per RFC 4253	SSH This port is used by 5620 SAM for an optional rsync feature between 5620 SAM Databases
	1523	TCP	Static Encryption Encryption provided by RC4 Cipher Algorithm with 128 bit Cipher Strength.	Oracle SQL*Net Listener This port is used by the 5620 SAM Server to connect to and communicate with the 5620 SAM Database. When there are redundant databases, this port is also used by Oracle DataGuard to keep the databases in sync. The data on this port is encrypted.
	9002 Ports from 32768 - 65536	TCP	None.	5620 SAM Database Proxy This port is used by the 5620 SAM Server to monitor disk usage on a remote 5620 SAM Database. When there are redundant databases, it is also allows the 5620 SAM Server to initiate database switchovers and failovers. Ports are allocated dynamically and temporarily in the range to satisfy the initial requests that arrive on port 9002 (the listener port).
	9003 Ports from 32768 - 65536	TCP	None.	Database file transfer Port This port is used by the 5620 SAM Database workstations in a redundant workstation configuration. This port allows Database transfers between the primary and standby databases. For example: when the standby database is re-instantiated, or when the standby database is installed for the first time. Ports are allocated dynamically and temporarily in the range to satisfy the initial requests that arrive on port 9003 (the listener port).
5620 SAM Client and Client Delegate	21 Ports from 1023 - 65536	TCP	None.	FTP (Passive) This port is used to enable ftp communication between the 5620 SAM Server and the managed routers. Ftp occurs to transfer information from the routers to the 5620 SAM Server such as accounting statistics. See section 8.7 for a more detailed description of ftp requirements.
	5510	UDP	None.	Trap Trap port used by 9500 MPR devices to send traps to SAM Clients running the NetO manager.

(6 of 6)

8.7 FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network

5620 SAM Server and 5620 SAM Auxiliary Statistics Collector will use FTP for several purposes.

The 5620 SAM Server will use FTP to receive backup images of managed devices, to send new software images to the managed devices and to receive accounting statistics from the managed devices.

If a 5620 SAM Auxiliary Statistics Collector workstation is installed, FTP will only be used to retrieve accounting statistics from managed devices.

If STM Accounting tests are being executed, the 5620 SAM Server will retrieve the test results from the managed devices by FTP.

The FTP communication is configured as an extended *passive* FTP connection, with the managed devices serving as the FTP servers and the 5620 SAM Server and 5620 SAM Auxiliary acting as the FTP client.

Extended passive FTP connections use dynamically-allocated ports on both sides of the communication channel, and are ephemeral in nature. As such, the data sent from the managed devices will be sent from a port in the range of 1024-65536. This data will be sent to the 5620 SAM Server on a port in the range of 1024-65536. Support for EPSV/EPRT ftp commands (commands that can replace PASV/PORT commands) must be enabled for connections to the 7x50 family of routers.

8.8 Firewall and NAT rules

Firewall rules are applied to the incoming network interface traffic of the 5620 SAM workstations. As a rule, firewall rules are not applied to the outgoing network interface traffic.

It is imperative that all rules are considered completely for the 5620 SAM systems to interoperate correctly. The following tables will define the rules to be applied to each 5620 SAM workstation. Within the section there will be a number of conditions that indicate whether or not that particular table needs to be applied.

5620 SAM Server firewall and NAT rules

When there is a firewall at the 5620 SAM Server(s) interface that reaches the managed network (NIC 2 on Figure 9-2), the following firewall rules need to be applied.

Table 8-2 SNMP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
UDP	Any	Managed Network	162	Server(s)	SNMP trap initiated from the NE
UDP	>32768	Server(s)	161	Managed Network	SNMP request
TCP	Any	Server(s)	8001	Managed Network	SNMP for 9471 MME
UDP	161	Managed Network	> 32768	Server(s)	SNMP response



Note — Due to the size of SNMP packets, IP fragmentation may occur in the network. Ensure the firewall will allow fragmented packets to reach the server(s).

Table 8-3 Telnet / FTP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
TCP	>32768	Server(s)	23	Managed Network	Telnet request
TCP	23	Managed Network	> 32768	Server(s)	Telnet response
TCP	Any	Server(s)	21	Managed Network	FTP requests (example: STM, Accounting Statistics, NE backups)
TCP	21	Managed Network	Any	Server(s)	FTP responses
TCP	> 1023	Managed Network	> 1023	Server(s)	Passive FTP ports for data transfer

Table 8-4 SSH / SFTP / SCP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
TCP	Any	Server(s)	22	Managed Network	SAM SSH request
TCP	22	Managed Network	Any	Server(s)	SAM SSH response
TCP	Any	Managed Network	22	Server(s)	eNodeB SFTP request
TCP	22	Server(s)	Any	Managed Network	eNodeB SFTP response
TCP	> 32768	Server(s)	830	Managed Network	SSH request for eNodeB
TCP	830	Managed Network	> 32768	Server(s)	SSH response for eNodeB
TCP	> 32768	Server(s)	830	Managed Network	SSHv2 request for MME
TCP	830	Managed Network	> 32768	Server(s)	SSHv2 response for MME

Table 8-5 7250 SAS or Telco T5C Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
UDP	Any	7250 SAS or Telco T5C	69	Server(s)	TFTP initiated by NE
UDP	Any	7250 SAS or Telco T5C	Any	Server(s)	TFTP transfer

Table 8-6 Other Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
ICMP	N/A	Managed Network	N/A	Server(s)	Only used if Ping Policy is enabled.
TCP	5001	7701 CPAA Elements	> 32768	Server(s)	

When there is a firewall at the interface that reaches the 5620 SAM Client(s) (NIC 3 on Figure 9-2) the following rules need to be applied.

Table 8-7 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Client(s) (GUI/OSS)

Protocol	From port	On	To port	On	Notes
TCP	Any	SAM-O Client	21	Server(s)	If FTP is required
TCP	Any	SAM-O Client	22	Server(s)	If SFTP/SCP is required
TCP	> 1023	SAM-O Client	> 1023	Server(s)	If FTP is required
TCP	Any	SAM-O/SAM GUI Client	1096-1097	Server(s)	JMS
TCP	Any	SAM-O/SAM GUI Client	1098	Server(s)	JNDI
TCP	Any	SAM-O/SAM GUI Client	1099	Server(s)	JNDI
TCP	Any	SAM GUI Client	4444,4450	Server(s)	JBoss
TCP	Any	SAM-O/SAM GUI Client	4446-4447	Server(s)	JMS
UDP	Any	SAM GUI Client	6100-6119	Server(s)	NEM Proxy
TCP	Any	SAM-O Client	8080	Server(s)	HTTP
TCP	Any	SAM GUI Client	8085	Server(s)	HTTP
TCP	Any	SAM GUI Client	8400	Server(s)	HTTP
TCP	Any	SAM-O/SAM GUI Client	8093, 8094	Server(s)	JMS
TCP	Any	SAM-O Client	8443	Server(s)	HTTPS
TCP	Any	SAM GUI Client	8444	Server(s)	HTTPS
TCP	Any	SAM GUI Client	9400	Server(s)	HTTPS
TCP	Any	SAM-O 3GPP-compliant Client	9735	Server(s)	Corba

When there is a firewall at the interface that reaches the 5620 SAM Client(s) (NIC 3 on Figure 9-2) AND redundant 5620 SAM Servers are used the following rules need to be applied. Configuration needs to be in both directions to handle an activity switch.

Table 8-8 5620 SAM Server interface to Client firewall rules for setups with redundant 5620 SAM Servers

Protocol	From port	On	To port	On
TCP	Any	Client	1100	Servers

When there is a firewall configured, and there are redundant 5620 SAM Servers, the following rules need to be applied to the appropriate interface. If multiple interfaces are used for communication to the clients (GUI and OSS) and auxiliary servers, the network traffic from the 5620 SAM Servers and 5620 SAM Auxiliaries could pass through the SAM client interface (NIC 3 on Figure 9-2) or the SAM network interface (NIC 1 on Figure 9-2) on the 5620 SAM Server. Configuration needs to be in both directions to handle an activity switch.

Table 8-9 5620 SAM Server-to-Server firewall rules for setups with redundant 5620 SAM Servers

Protocol	From port	On	To port	On
TCP	Any	Servers	1098	Servers
TCP	Any	Auxiliary Servers	1100	Servers
TCP	Any	Servers	1100	Servers

When there is a firewall configured, and there are redundant 5620 SAM Auxiliary workstation(s), the following rules need to be applied to the appropriate interface. If multiple interfaces are used for communication to the clients (GUI and OSS) and auxiliary servers, the network traffic from the 5620 SAM Servers and 5620 SAM Auxiliaries could pass through the SAM client interface (NIC 3 on Figure 9-2) or the SAM network interface (NIC 1 on Figure 9-2) on the 5620 SAM Server.

Table 8-10 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Auxiliary Server(s)

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	1096-1097	Server(s)
TCP	Any	Auxiliary Server(s)	1098	Server(s)
TCP	Any	Auxiliary Server(s)	1099	Server(s)
TCP	Any	Auxiliary Server(s)	4444	Server(s)
TCP	Any	Auxiliary Server(s)	4446-4447	Server(s)
TCP	Any	Auxiliary Server(s)	4450	Server(s)
TCP	Any	Auxiliary Server(s)	8093	Server(s)
TCP	Any	Auxiliary Server(s)	8094	Server(s)

When a firewall and NAT are configured to the 5620 SAM Server at the SAM client interface (NIC 3 on Figure 9-2) the following rules need to be applied to allow the OSS clients to retrieve the logToFile accounting statistics information. Services require the use of public addresses.

Table 8-11 Additional firewall rules required to allow services on the 5620 SAM client(s) to communicate with the 5620 SAM Server if NAT is used.

Protocol	From port	On	To port	On
TCP	Any	Server Public Address	21	Server Private Address
TCP	21	Server Public Address	Any	Server Private Address
TCP	> 1023	Server Public Address	> 1023	Server Private Address

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 9-2), the following rules apply.

Table 8-12 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Database Server(s)

Protocol	From port	On	To port	On
TCP	1523	Database Server(s)	Any	Server(s)
TCP	9002	Database Server(s)	Any	Server(s)
TCP	> 32768	Database Server(s)	> 32768	Server(s)

When there is a firewall at the SAM management interface (NIC 1 on Figure 9-2) and 5620 SAM Server redundancy is configured, then the following rules need to be applied. Configuration needs to be in both directions to handle an activity switch.

Table 8-13 Firewall rules for setups with redundant 5620 SAM Servers.

Protocol	From port	On	To port	On
TCP	Any	Servers	22	Servers
TCP	22	Servers	Any	Servers
TCP	Any	Servers	9010	Servers
TCP	Any	Servers	11800	Servers
TCP	11800	Servers	Any	Servers
TCP	Any	Servers	12300-12307	Servers
TCP	12300-12307	Servers	Any	Servers
TCP	> 32768	Servers	> 32768	Servers

When there is a firewall at the SAM management interface (NIC 1 on Figure 9-2) and 5620 SAM Auxiliary Servers are configured, then the following rules need to be applied:

Table 8-14 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Auxiliary Server(s).

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	12300-12307	Server(s)
TCP	12300-12307	Auxiliary Server(s)	Any	Server(s)
TCP	Any	Auxiliary Server(s)	12800	Server(s)
TCP	12800	Auxiliary Server(s)	Any	Server(s)

When there is a firewall at the SAM management interface (NIC 1 on Figure 9-2) and NAT is configured, then the following rules need to be applied. Services require the use of public addresses.

5620 SAM Database firewall and NAT rules

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 9-2), the following rules apply.

Table 8-15 Firewall rules for traffic coming into the 5620 SAM Database Server(s) from the 5620 SAM Server(s) and 5620 SAM Auxiliary Server(s)

Protocol	From port	On	To port	On
TCP	Any	Server(s) & Auxiliary Server(s)	1523	Database Server(s)
TCP	Any	Server(s) & Auxiliary Server(s)	9002	Database Server(s)
TCP	> 32768	Server(s) & Auxiliary Server(s)	> 32768	Database Server(s)

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 9-2) and redundancy is configured, the following rules apply. Configuration needs to be in both directions to handle an activity switch.

Table 8-16 Firewall rules for traffic between the 5620 SAM Database Servers (redundant only)

Protocol	From port	On	To port	On
TCP	Any	Database Servers	22	Database Servers
TCP	22	Database Servers	Any	Database Servers
TCP	Any	Database Servers	1523	Database Servers
TCP	1523	Database Servers	> 32768	Database Servers
TCP	Any	Database Servers	9002 >32768	Database Servers Ports are allocated dynamically and temporarily in the range to satisfy the initial requests that arrive on port 9002.

(1 of 2)

Protocol	From port	On	To port	On
TCP	9002	Database Servers	> 32768	Database Servers
TCP	Any	Database Servers	9003 > 32768	Database Servers Ports are allocated dynamically and temporarily in the range to satisfy the initial requests that arrive on port 9003.
TCP	9003	Database Servers	> 32768	Database Servers

(2 of 2)

5620 SAM Auxiliary Server firewall and NAT rules

When there is a firewall at the interface that reaches the managed network (NIC 2 on Figure 9-2), the following rules apply.

Table 8-17 SNMP Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
UDP	>32768	Auxiliary Server(s)	161	Managed Network	SNMP request
UDP	161	Managed Network	> 32768	Auxiliary Server(s)	SNMP response



Note — Due to the size of SNMP packets, IP fragmentation may occur in the network. Ensure the firewall will allow fragmented packets to reach the server(s).

Table 8-18 SSH / Telnet Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
TCP	>32768	Auxiliary Server(s)	22-23	Managed Network	SSH/SCP/Telnet request
TCP	22-23	Managed Network	> 32768	Auxiliary Server(s)	SSH/SCP/Telnet response

Table 8-19 SNMP FTP Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
TCP	Any	Auxiliary Server(s)	21	Managed Network	FTP requests (example: STM, Accounting statistics, NE backups))
TCP	21	Managed Network	Any	Auxiliary Server(s)	FTP responses
TCP	> 1023	Managed Network	> 1023	Auxiliary Server(s)	Passive FTP ports for data transfer (See Section 8.7)



Note — FTP access is only required for the 5620 SAM Auxiliary Statistics Collector.

Table 8-20 SNMP Firewall rules for traffic coming into the 5620 SAM Auxiliary Call Trace Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
UDP	> 32768	Auxiliary Server(s)	161	Managed Network	SNMP request
UDP	161	Managed Network	> 32768	Auxiliary Server(s)	SNMP response



Note — Due to the size of SNMP packets, IP fragmentation may occur in the network. Ensure the firewall will allow fragmented packets to reach the server(s).

Table 8-21 Call Trace Data Firewall rules for traffic coming into the 5620 SAM Auxiliary Call Trace Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
UDP	Any	Managed Network	57074,57075	Auxiliary Server(s)	Call Trace Data

When there is a firewall at the interface that reaches the 5620 SAM Client(s) (NIC 3 on Figure 9-2), the following rules apply for FTP access to the 5620 SAM Auxiliary by the OSS Client.

Table 8-22 Firewall rules for OSS Client communication to the 5620 SAM Auxiliary Server(s)

Protocol	From port	On	To port	On	Notes
TCP	21	SAM-O Client	Any	Auxiliary Server(s)	FTP requests (logToFile statistics, and call trace information)
TCP	Any	SAM-O Client	21	Auxiliary Server(s)	FTP responses
TCP	> 1023	SAM-O Client	Any	Auxiliary Server(s)	Passive FTP ports for data transfer (See Section 8.7)
Only for 5620 SAM Auxiliary Call Trace Collectors					
TCP	Any	SAM-O 3GPP-compliant Client	9735	Auxiliary Server(s)	Corba interface to access Call Trace information

When there is a firewall at the interface that communicates with the 5620 SAM Servers, the following rules apply for inter process communication. If multiple interfaces are used for 5620 SAM Server communication to the clients (GUI and OSS) and auxiliary servers, the network traffic from the 5620 SAM Auxiliaries could pass through the SAM client interface (NIC 3 on Figure 9-2) or the SAM network interface (NIC 1 on Figure 9-2) of the 5620 SAM Auxiliary.

Table 8-23 Firewall rules for inter process communication on the 5620 SAM Auxiliary Server(s)

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	1094-1095	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	4448	Auxiliary Server(s)

When there is a firewall at the interface that communicates with the 5620 SAM Servers, the following rules apply. If multiple interfaces are used for 5620 SAM Server communication to the clients (GUI and OSS) and auxiliary servers, the network traffic from the 5620 SAM Auxiliaries could pass through the SAM client interface (NIC 3 on Figure 9-2) or the SAM network interface (NIC 1 on Figure 9-2) of the 5620 SAM Auxiliary.

Table 8-24 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Server(s)

Protocol	From port	On	To port	On
TCP	1096-1097	Server(s)	Any	Auxiliary Server(s)
TCP	1098	Server(s)	Any	Auxiliary Server(s)
TCP	1099	Server(s)	Any	Auxiliary Server(s)
TCP	4444	Server(s)	Any	Auxiliary Server(s)
TCP	4446-4447	Server(s)	Any	Auxiliary Server(s)

(1 of 2)

Protocol	From port	On	To port	On
TCP	4450	Server(s)	Any	Auxiliary Server(s)
TCP	8093	Server(s)	Any	Auxiliary Server(s)
TCP	8094	Server(s)	Any	Auxiliary Server(s)
TCP	> 32768	Server(s)	> 32768	Auxiliary Server(s)

(2 of 2)

When there is a firewall at the interface that communicates with the 5620 SAM Server and 5620 SAM Server redundancy is configured, the following rules apply. If multiple interfaces are used for 5620 SAM Server communication to the clients (GUI and OSS) and auxiliary servers, the network traffic from the 5620 SAM Auxiliaries could pass through the SAM client interface (NIC 3 on Figure 9-2) or the SAM network interface (NIC 1 on Figure 9-2) of the 5620 SAM Auxiliary.

Table 8-25 Firewall rules for setups with redundant 5620 SAM Servers

Protocol	From port	On	To port	On
TCP	1100	Server(s)	Any	Auxiliary Server(s)

When there is a firewall at the interface that reaches the 5620 SAM Client(s) (NIC 3 on Figure 9-2) and NAT is used on the 5620 SAM Auxiliary Server(s), the following rules apply to allow the OSS clients to collect the logToFile accounting statistics files. Services require the use of public addresses.

Table 8-26 Additional Firewall rules required to allow services on the 5620 SAM client(s) to communicate with the 5620 SAM Auxiliary(s) if NAT is used on the Auxiliary Server(s).

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server Public Address	21	Auxiliary Server Private Address
TCP	21	Auxiliary Server Public Address	Any	Auxiliary Server Private Address
TCP	> 1023	Auxiliary Server Public Address	> 1023	Auxiliary Server Private Address

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 9-2), the following rules apply.

Table 8-27 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Database Server(s)

Protocol	From port	On	To port	On
TCP	1523	Database Server(s)	Any	Auxiliary Server(s)
TCP	9002	Database Server(s)	Any	Auxiliary Server(s)

(1 of 2)

Protocol	From port	On	To port	On
TCP	> 32768	Database Server(s)	> 32768	Auxiliary Server(s)

(2 of 2)

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 9-2), the following rules apply.

Table 8-28 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Server(s)

Protocol	From port	On	To port	On
TCP	Any	Server(s)	12300-12307	Auxiliary Server(s)
TCP	12300-12307	Server(s)	Any	Auxiliary Server(s)
TCP	Any	Server(s)	12800	Auxiliary Server(s)
TCP	12800	Server(s)	Any	Auxiliary Server(s)

Table 8-29 Firewall rules for traffic between redundant 5620 SAM Auxiliary Statistics Collector Servers.

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Statistics Collector	22	Auxiliary Statistics Collector
TCP	Any	Auxiliary Statistics Collector	9010	Auxiliary Statistics Collector

Table 8-30 Firewall rules for traffic between redundant 5620 SAM Auxiliary Call Trace Collector Servers.

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Call Trace Collector	9010	Auxiliary Call Trace Collector

5620 SAM Server to delegate workstation

Ensure that ICMP protocol traffic from the 5620 SAM Server workstation(s) can reach the 5620 SAM delegate workstation.

5620 SAM Client to managed network communications

Apply the following changes to the connection between the 5620 SAM Client and the managed network. Note that all connections are bi-directional.

Table 8-31 Firewall rules for traffic between the 5620 SAM Client and the 5780 DSC

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	443	Managed Network	HTTPS

Table 8-32 Firewall rules for traffic between the 5620 SAM Client and the 9471 MME

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client (s)	1099	Managed Network	RMI
TCP	Any	5620 SAM Client (s)	1234	Managed Network	Search-agent
TCP	Any	5620 SAM Client (s)	1235	Managed Network	Search-agent
TCP	Any	5620 SAM Client (s)	4567	Managed Network	tram
TCP	Any	5620 SAM Client (s)	8443	Managed Network	HTTPS
TCP	Any	5620 SAM Client (s)	9683	Managed Network	HTTPS

Table 8-33 Firewall rules for traffic between the 5620 SAM Client and the eNodeB NEM

Protocol	From port	On	To port	On	Notes
UDP	Any	5620 SAM Client(s)	161	Managed Network	SNMP
TCP	Any	5620 SAM Client(s)	830	Managed Network	NetConf over SSH

Table 8-34 Firewall rules for traffic between the 5620 SAM Client and GNEs

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	80/8080	Managed Network	HTTP (See GNE vendor for specifics)
TCP	Any	5620 SAM Client(s)	443/8443	Managed Network	HTTPS (See GNE vendor for specifics)

Table 8-35 Firewall rules for traffic between the 5620 SAM Client and 9500 MPR NetO

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	21	Managed Network	FTP (MSS-8/4 and AWY variants only)

(1 of 2)

Protocol	From port	On	To port	On	Notes
TCP	21	5620 SAM Client	Any	Managed Network	FTP
TCP	Any	5620 SAM Client(s)	80	Managed Network	HTTP
UDP	Any	5620 SAM Client(s)	161	Managed Network	SNMP
TCP	>1023	5620 SAM Client(s)	Any	Managed Network	Passive FTP (MSS-8/4 and AWY variants only)
TCP	Any	5620 SAM Client(s)	>1023	Managed Network	Passive FTP
UDP	5510	5620 SAM Client(s)	5510	Managed Network	SNMP Traps for 9500 MSS-8/4 chassis type
UDP	5510	5620 SAM Client	Any	Managed Network	SNMP Traps for 9500 MSS-1C, MPR-e, and 9400AWY chassis type
UDP	Any	5620 SAM Client	11500	Managed Network	MSS-1C and MPR-e variants only

(2 of 2)

Table 8-36 Firewall rules for traffic between the 5620 SAM Client and Omni Switches

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	80	Managed Network	HTTP
TCP	Any	5620 SAM Client(s)	443	Managed Network	HTTPS

9 — *Deploying 5620 SAM with multiple network interfaces/IP addresses*

- 9.1 Deploying 5620 SAM with multiple network interfaces/IP addresses 9-2
- 9.2 5620 SAM Server multiple IP addresses deployment scenarios 9-2
- 9.3 5620 SAM Auxiliary Statistics Collector multiple IP addresses deployment scenarios 9-3
- 9.4 5620 SAM Auxiliary Call Trace Collector multiple IP addresses deployment scenarios 9-4
- 9.5 Using Network Address Translation 9-7
- 9.6 Configuring 5620 SAM Server to utilize multiple network interfaces 9-9
- 9.7 Use of hostnames for the 5620 SAM Client 9-9

9.1 Deploying 5620 SAM with multiple network interfaces/IP addresses

The 5620 SAM Server and 5620 SAM Auxiliary components of the application communicate with very different entities: a managed network, a collection of Clients (GUIs and OSS), and between each other. Since these entities usually exist in very different spaces, Alcatel-Lucent recognizes the importance of separating these different types of traffic. Alcatel-Lucent therefore supports configuring the 5620 SAM Server and 5620 SAM Auxiliary such that it uses different network interfaces (IP addresses) to manage the network and to service the requirements of the 5620 SAM Clients.

5620 SAM Server uses an internal communications system (JGroups/JMS) to handle bi-directional access to the 5620 SAM Server for the 5620 SAM Clients and the 5620 SAM Auxiliary servers. In 5620 SAM Release 9.0, this communication system can be configured to allow the 5620 SAM Clients and 5620 SAM Auxiliaries to communicate using different network interfaces on the 5620 SAM Server. This adds significant flexibility when isolating the different types of traffic to the 5620 SAM Server. If using this mode, special attention must be paid to the firewall rules on the network interfaces on the 5620 SAM Server and 5620 SAM Auxiliary (NICs 1 and NICs 3 on Figure 9-2).

Deploying a 5620 SAM Server and 5620 SAM Auxiliary with multiple IP addresses is only supported when the 5620 SAM Server is installed on Solaris.

When installing 5620 SAM components on workstations with multiple interfaces, each interface must reside on a separate subnet, with the exception of interfaces that are to be used in an IPMP group.

9.2 5620 SAM Server multiple IP addresses deployment scenarios

The 5620 SAM Server supports the configuration of different IP addresses for the following purposes:

- One network interface can be used to manage the network. (NIC 2 on Figure 9-2) This network interface contains the IP address that the managed devices will use to communicate with the 5620 SAM Server and 5620 SAM Auxiliary. All managed devices must be configured to use the same IP address to communicate to the 5620 SAM Server.
- One network interface can be used to service the requirements of the 5620 SAM clients (GUIs and OSS) (NIC 3 on Figure 9-2). This network interface contains the IP address that all clients (GUIs and OSS) will use to communicate with the 5620 SAM Server. All clients (GUIs and OSS) must be configured to use the same IP address to communicate to the 5620 SAM Server. This IP address can be different from the one used by the managed devices to communicate with the 5620 SAM Server.
- One network interface can be used to communicate with the 5620 SAM Database as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 9-2). This network interface contains the IP address that the 5620 SAM Database and redundant 5620 SAM components will use to communicate with

the 5620 SAM Server. This IP address can be different from the addresses used by the 5620 SAM clients and the managed devices to communicate with the 5620 SAM Server.

- In a redundant 5620 SAM installation, the 5620 SAM Servers and 5620 SAM Auxiliary must have IP connectivity to the 5620 SAM Server peer. If multiple interfaces are used for communication to the clients and auxiliary servers, the connectivity required could be to the client interface (NIC 3 on Figure 9-2) or the database/server interface (NIC 1 on Figure 9-2).
- Additional network interfaces may be configured on the 5620 SAM Server workstation, at the customer's discretion, to perform maintenance operations such as workstation backups.
- IPv4 and IPv6 network elements can be managed from the same interface or from separate interfaces. (NIC3 and/or NIC4 on Figure 9-2).

9.3 5620 SAM Auxiliary Statistics Collector multiple IP addresses deployment scenarios

The 5620 SAM Auxiliary Statistics Collector supports the configuration of different IP addresses for the following purposes:

- One network interface can be used to retrieve information from the managed network. (NIC 2 on Figure 9-2) This network interface contains the IP address that the managed devices will use to retrieve the accounting statistics files from the network elements.
- One network interface can be used to service the requirements of the OSS clients (NIC 3 on Figure 9-2). This network interface contains the IP address that all OSS clients will use to communicate with the 5620 SAM Auxiliary Statistics Collector. OSS Clients will use this IP address to retrieve the logToFile statistics collection data from the 5620 SAM Auxiliary Statistics Collector.
- One network interface can be used to communicate with the 5620 SAM Database as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 9-2). This network interface contains the IP address that the 5620 SAM Database and redundant 5620 SAM components will use to communicate with the 5620 SAM Server. This IP address can be different from the addresses used by the 5620 SAM OSS clients and the managed devices to communicate with the 5620 SAM Server.
- In a redundant 5620 SAM installation, the 5620 SAM Auxiliary Statistics Collector must have IP connectivity to the 5620 SAM Server peer. If multiple interfaces are used for the 5620 SAM Server to communicate to the clients and auxiliary servers, the connectivity required could be to the client interface (NIC 3 on Figure 9-2) or the database/server interface (NIC 1 on Figure 9-2).
- Additional network interfaces may be configured on the 5620 SAM Auxiliary Statistics Collector workstation, at the customer's discretion, to perform maintenance operations such as workstation backups.
- IPv4 and IPv6 network elements can be managed from the same interface or from separate interfaces. (NIC3 and/or NIC4 on Figure 9-2).

9.4 5620 SAM Auxiliary Call Trace Collector multiple IP addresses deployment scenarios

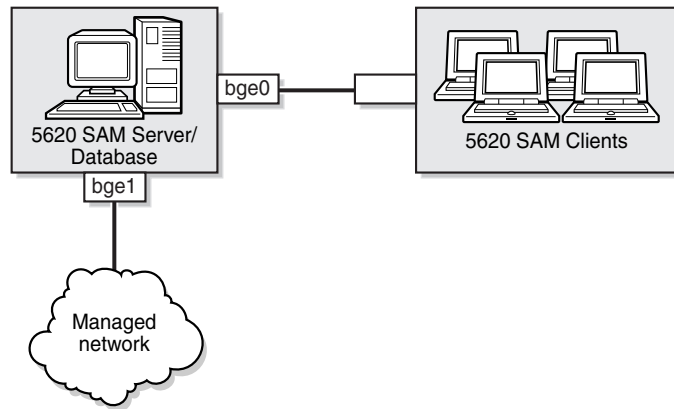
The 5620 SAM Auxiliary Call Trace Collector supports the configuration of different IP addresses for the following purposes:

- One network interface can be used to retrieve information from the managed network. (NIC 2 on Figure 9-2) This network interface contains the IP address that the managed devices will use to send the call trace messages from the network elements.
- One network interface can be used to service the requirements of the 9958 WTA client (NIC 3 on Figure 9-2). This network interface contains the IP address that all clients will use to communicate with the 5620 SAM Auxiliary Call Trace Collector. 9958 WTA will use this IP address to retrieve the Call Trace data from the 5620 SAM Auxiliary Call Trace Collector.
- One network interface can be used to communicate with the 5620 SAM management complex as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 9-2). This network interface contains the IP address that the 5620 SAM management complex components will use to communicate with the 5620 SAM Auxiliary Call Trace Collector. If a redundant 5620 SAM Auxiliary Call Trace Collector is present, this network interface will also be used to sync Call Trace and Debug Trace data collected from the network, with the peer 5620 SAM Auxiliary Call Trace Collector. This IP address can be different from the addresses used by the 9958 WTA clients and the managed devices to communicate with the 5620 SAM Server.
- In a redundant 5620 SAM installation, the 5620 SAM Auxiliary Call Trace Collector must have IP connectivity to the 5620 SAM Server peer. If multiple interfaces are used for the 5620 SAM Server to communicate to the clients and auxiliary servers, the connectivity required could be to the client interface (NIC 3 on Figure 9-2 or the database/server interface (NIC 1 on Figure 9-2).
- Additional network interfaces may be configured on the 5620 SAM Auxiliary Call Trace Collector workstation, at the customer's discretion, to perform maintenance operations such as workstation backups.
- IPv4 and IPv6 network elements can be managed from the same interface or from separate interfaces. (NIC3 and/or NIC4 on Figure 9-2).

It is not necessary to use the first network interface on the 5620 SAM Server workstation (i.e. ce0, bge0) to communicate with the 5620 SAM GUI Clients.

Figure 9-1 illustrates a collocated 5620 SAM Server/Database deployment where the 5620 SAM Server is configured to actively use more than one network interface.

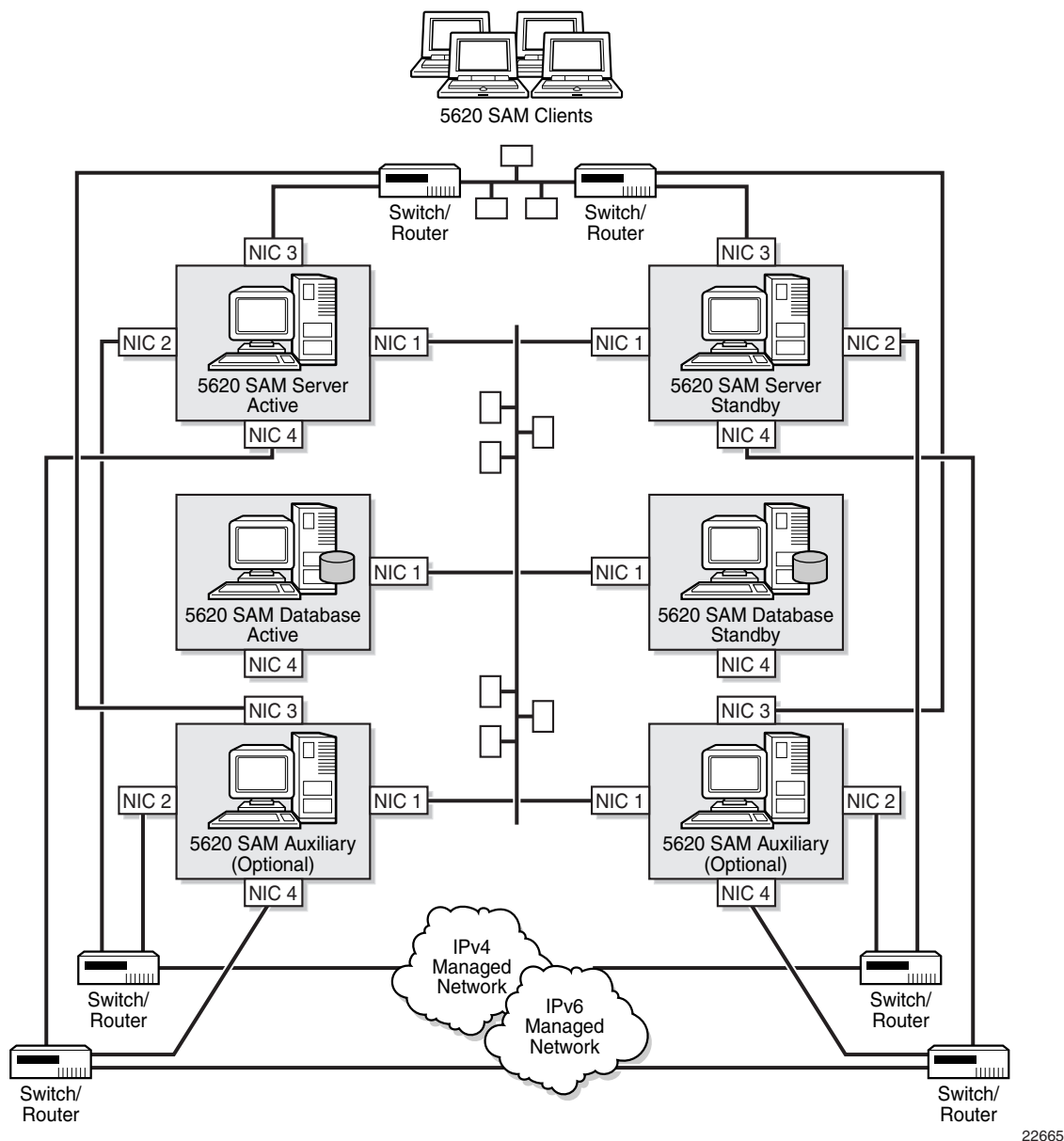
Figure 9-1 Collocated 5620 SAM Server/Database deployment with multiple network interfaces



22666

Figure 9-2 illustrates a distributed, redundant 5620 SAM deployment where the 5620 SAM Servers are configured to actively use more than one network interface.

Figure 9-2 Distributed 5620 SAM Server/Database deployment with multiple network interfaces



Due to limitations with the inter-process and inter-workstation communication mechanisms, a specific network topology and the use of hostnames may be required (see section 9.7). Contact an Alcatel-Lucent representative to obtain further details.

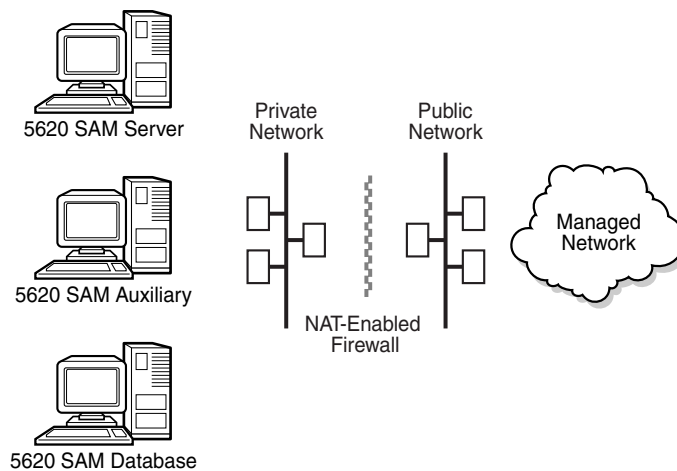
9.5 Using Network Address Translation

5620 SAM supports the use of Network Address Translation (NAT) between the following components:

- The 5620 SAM Server and 5620 SAM Clients (GUIs or OSS)
- The 5620 SAM Server and the managed network
- The 5620 SAM Auxiliary and the managed network

Figure 9-3 illustrates a deployment of 5620 SAM where NAT is used between the 5620 SAM Server and the managed network.

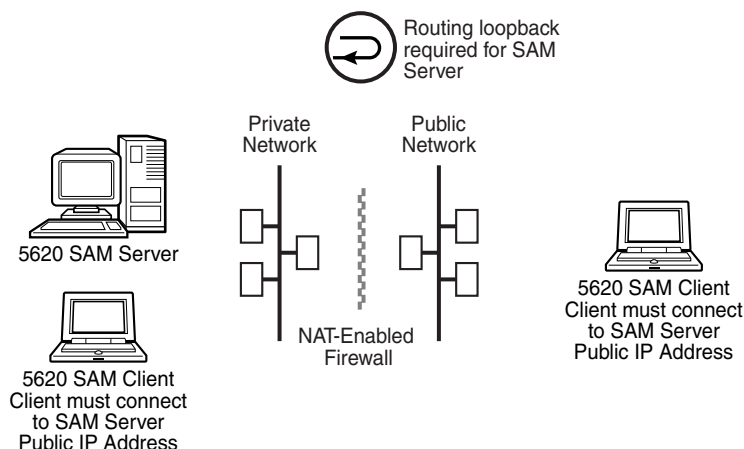
Figure 9-3 5620 SAM Server deployments with NAT between the Server and the managed network



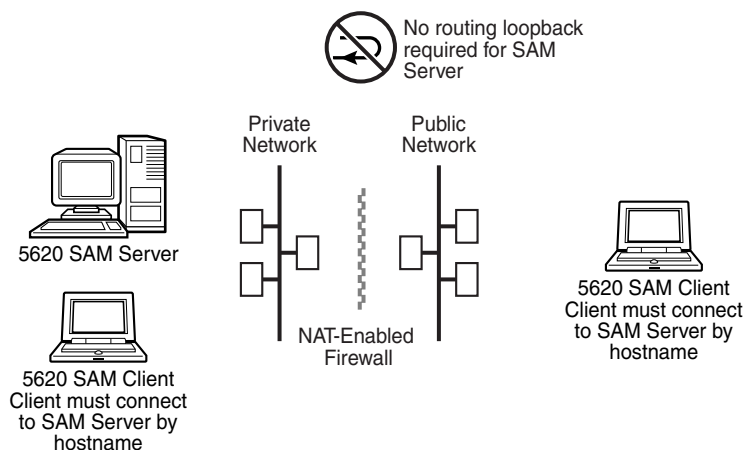
22664

The following two figures illustrate a deployment of 5620 SAM where NAT is used between the 5620 SAM Server and the 5620 SAM Clients (GUIs, OSS or Client Delegates). In figure 9-4, SAM Clients on the private side and public side of the NAT-Enabled Firewall must connect to the public IP address of the SAM Server. A routing loopback from the SAM Server private IP address to the SAM Server public IP address must be configured in this scenario as all SAM Clients must communicate to the SAM Server through the SAM Server public IP address.

The 5620 SAM Auxiliary will need to be able to connect to the public IP address of the 5620 SAM server.

Figure 9-4 NAT'd 5620 SAM Server deployment with IP Address communication

22663

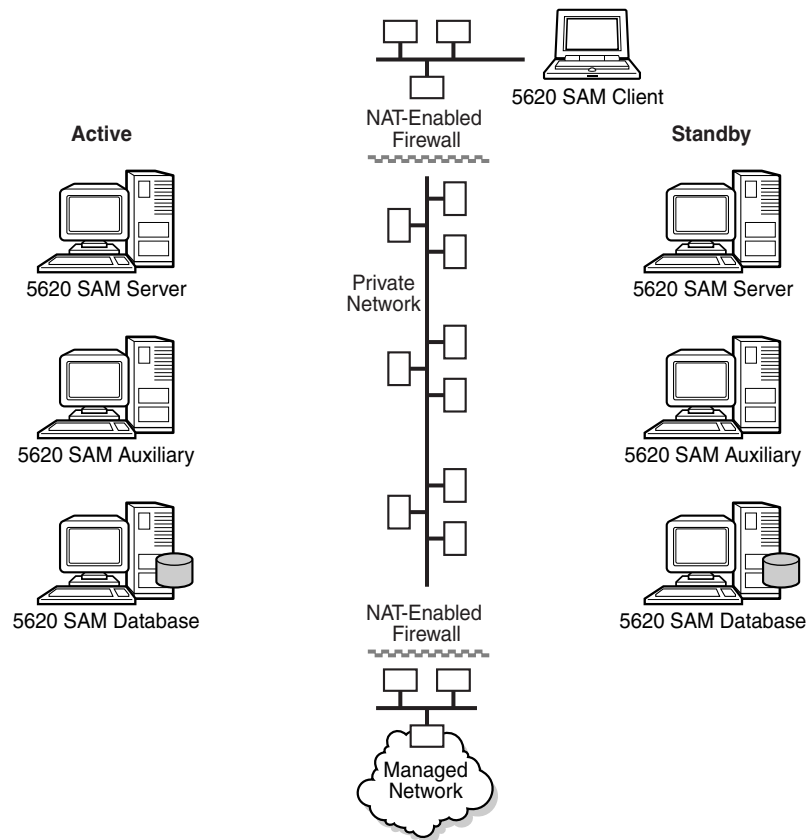
Figure 9-5 NAT'd 5620 SAM Server deployment with Name Resolution based communication

22662

In Figure 9-5, a name resolution service on the public side of the NAT-Enabled Firewall is configured to resolve the SAM Server hostname to the public IP address of the SAM server. Name resolution service on the private side of the NAT-Enabled Firewall is configured to resolve the SAM Server hostname to the private IP address of the SAM server. Clients on both sides of the NAT-Enabled Firewall are configured to communicate with the SAM Server via hostname where the SAM Server hostname must be the same on both sides of the NAT-Enabled Firewall.

Figure 9-6 illustrates a deployment of 5620 SAM where NAT is used between the 5620 SAM complex, 5620 SAM clients, and the managed network.

Figure 9-6 5620 SAM deployment with NAT



22661

NAT rules must be in place before 5620 SAM installation can occur, since the installation scripts will access other systems for configuration purposes.

9.6 Configuring 5620 SAM Server to utilize multiple network interfaces

The configuration of the 5620 SAM Server application to use multiple interfaces is done at installation time. At that time, the installation utility prompts the user to enter the IP addresses of the various network interfaces that are to be used within the 5620 SAM network management complex.

9.7 Use of hostnames for the 5620 SAM Client

There are a number of situations where it is necessary for the 5620 SAM Client to be configured to use a hostname rather than a fixed IP address to reach the 5620 SAM Server.

For situations where the 5620 SAM Server's public address is exposed to multiple networks with different IP addresses, a hostname can be used instead of a fixed IP address. This is most useful when NAT is used between 5620 SAM clients and the 5620 SAM Server that can be accessed via multiple networks.

For situations where the 5620 SAM Client and the 5620 SAM Auxiliary are using different network interfaces to the 5620 SAM Server, the 5620 SAM Client must use a hostname to reach the 5620 SAM Server.

In both cases, a hostname can be used by configuring DNS, or by configuring the local host file to ensure that the hostname can be translated to an IP address.

This feature is available as of 5620 SAM Release 6.0 R4.

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



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

3HE 06557 AAAJ TQZZA Edition 01