



Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 6.0
SYSTEM ARCHITECTURE GUIDE

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 2008 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

About this document

The *5620 SAM System Architecture Guide* is intended for technology officers and network planners, to increase their knowledge of the 5620 SAM software structure and components.

The *5620 SAM System Architecture Guide* describes the system structure, software components, and interfaces of the 5620 Service Aware Manager. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.

About related documentation

There are several documents that describe the 5620 SAM and the managed devices.

- See the *5620 SAM Planning Guide* for information about 5620 SAM scalability and recommended hardware configurations.
- See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about installing the 5620 SAM database, server, and client software.
- See the *5620 SAM User Guide* for information about using the client GUI to perform network management functions.
- See the *5620 SAM Parameter Guide* for definitions, ranges, dependencies, and default values for configurable 5620 SAM client GUI parameters.
- See the *5620 SAM-O OSS Interface Developer Guide* for information about using the XML OSS interface to create OSS applications, for example, to perform alarm monitoring and inventory control.
- See the *5620 SAM Routine Maintenance Procedures Guide* for information about developing and scheduling regular maintenance activities.
- See the *5620 SAM System Architecture Guide* for information about software component interaction.
- See the *5620 SAM NE Compatibility Guide* for release-specific information about the compatibility of managed-device features with different 5620 SAM releases.
- See the *5620 SAM Statistics Management Guide* for information about managing 5620 SAM statistics collection and to view a list of the MIB counters that are available for collection using the 5620 SAM.
- See the index file in the User_Documentation directory on the application DVD for additional documentation information.

See the 7750 SR, 7450 ESS, 7710 SR, 7705 SAR, 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, OS 6850, and Telco user documentation for information about device-specific CLI commands, parameters, and installation. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

Procedure 1 To find the 5620 SAM user documentation

The user documentation is available from the following sources:

- The User_Documentation directory on the product DVD-ROM
 - Help→5620 SAM User Documentation in the 5620 SAM client GUI main menu
-

Multiple PDF document search

You can use Adobe Reader Release 6.0 and later to search multiple PDF files for a common term. Adobe Reader displays the results in a single display panel. The results are grouped by PDF file, and you can expand the entry for each file.



Note — The PDF files in which you search must be in the same folder.

Procedure 2 To search multiple PDF files for a common term

- 1 Open Adobe Acrobat Reader.
- 2 Choose Edit→Search from the Acrobat Reader main menu. The Search PDF panel appears.
- 3 Enter the search criteria.
- 4 Click on the All PDF Documents In radio button.
- 5 Select the folder in which to search using the drop-down menu.
- 6 Click on the Search button.

Acrobat Reader displays the search results. You can expand the entries for each document by clicking on the + symbol.

Contents

Preface	ix
About this document	ix
About related documentation.....	x
Procedure 1 To find the 5620 SAM user documentation.....	x
Multiple PDF document search.....	x
Procedure 2 To search multiple PDF files for a common term.....	xi
1 — 5620 SAM architecture	1-1
1.1 5620 SAM architecture overview.....	1-2
Benefits.....	1-2
1.2 5620 SAM components.....	1-3
Main components.....	1-3
Multi-tier model	1-3
Server data model	1-5
Distributed server architecture	1-5
1.3 Component interfaces.....	1-6
Servers and managed devices	1-6
Main server and clients.....	1-7
Main server and database.....	1-7
Main server and auxiliary servers.....	1-8
5620 SAM and external systems	1-8
1.4 Security	1-9
Session management.....	1-10
Network transport security	1-11
1.5 Fault tolerance	1-12
Main server and database redundancy.....	1-12
1.6 Network management capabilities	1-14
5620 SAM network-management functional areas	1-14
Service management	1-14
Billing	1-14

	Equipment management	1-15
	Performance management.....	1-15
	Fault management	1-15
1.7	Standards compliance	1-16

Glossary

Index

1 — 5620 SAM architecture

- 1.1 5620 SAM architecture overview 1-2**
- 1.2 5620 SAM components 1-3**
- 1.3 Component interfaces 1-6**
- 1.4 Security 1-9**
- 1.5 Fault tolerance 1-12**
- 1.6 Network management capabilities 1-14**
- 1.7 Standards compliance 1-16**

1.1 5620 SAM architecture overview

The 5620 SAM supports IP/MPLS-based network convergence by providing customer services such as VLL, VPLS, VPRN, IES, and VLAN over a common network infrastructure. The 5620 SAM allows network operators to manage their networks at the customer, service, and subscriber host levels.

The 5620 SAM software architecture is built on industry standards including open standards such as SOAP and XML, the Java and J2EE framework, multi-tier layering, and web service interfaces. This use of standard interfaces allows the 5620 SAM to integrate with other network management systems such as the 5620 NM and the 5750 SSC, to add management of IP/MPLS and metro Ethernet services to multiservice networks.

Benefits

Open standards, the multi-tier and web service models, and distributed server processing provide many benefits that include the following.

- Open standards are widely used and promote interoperability with other systems. The large industry knowledge base means that multiple resources are available for service creation and configuration.
- Distributed server processing using auxiliary servers spreads the server processing workload across multiple hardware components to provide greater efficiency in the execution of network-management tasks, for example, the collection of performance and accounting statistics data from managed devices.
- The multi-tier model packages functionality in separate, well-defined elements that can be coded quickly, easily maintained, and combined with different vendor product components. The scope of system changes are contained within components, which provides flexibility for future growth. To improve performance and scalability, different components can be spread over multiple processors or duplicated for multiprocessor execution.
- Web services are created when applications export their XML interfaces over the web, which allows remote components, including web portals, to access the services. The XML access to 5620 SAM functionality allows third-party vendors to create customized windows into 5620 SAM services.

1.2 5620 SAM components

The main 5620 SAM components can be viewed from a multi-tier perspective. These components are built using Alcatel-Lucent and non-Alcatel-Lucent software.

All licensed subcomponents of the 5620 SAM are listed in the 5620 SAM server directory `/nms/distribution/licenses`. The following is a partial list of licensed subcomponents. See the README files for each license for more information.

- Apache Software Foundation log4j
- Sun Microsystems JDK, Java, and JRE
- Oracle for Solaris and Oracle Enterprise
- Zero G Software InstallAnywhere
- Jboss Application Server
- AXL Radius and TACACS+
- SL Corp SL-GMS
- Sourceforge ganymed-ssh2

Main components

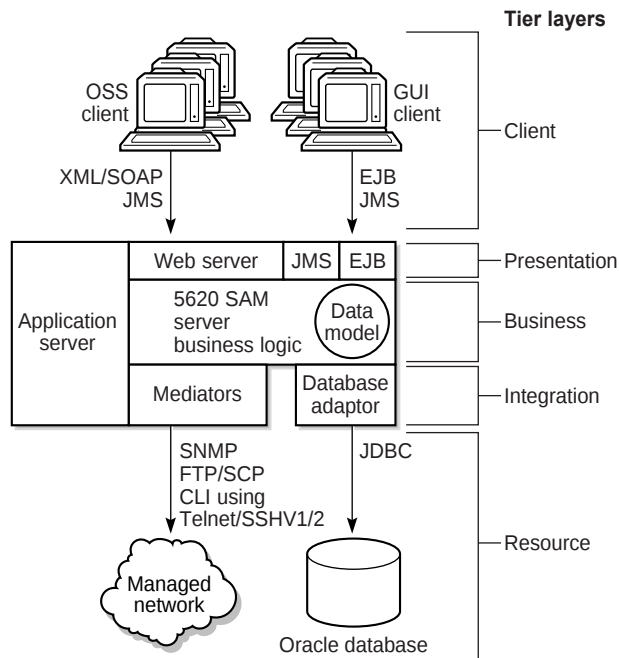
The following are the main components of a 5620 SAM system.

- The server is a network-management processing engine written in Java that runs on a Sun Solaris or Microsoft Windows platform. The server includes several third-party components, such as an application server, JMS server, web server, protocol stack set, and database adaptor. Server functionality can be concentrated on one physical platform, or distributed across multiple dedicated workstations.
- The database is a customized Oracle relational database that provides persistent storage for the network data. The database can run on the same station as the 5620 SAM main server software, or on a different station.
- The clients are OSS applications or Java-based 5620 SAM GUIs. The 5620 SAM GUIs run on Sun Solaris, Microsoft Windows, or Red Hat Linux platforms. The OSS applications can run on any platform, because they exchange platform-neutral XML/SOAP messages with the 5620 SAM main server. The 5620 SAM GUI and OSS clients do not communicate with auxiliary servers.

Multi-tier model

Figure 1-1 shows a five-layer multi-tier model of the 5620 SAM with the components at each layer.

Figure 1-1 5620 SAM multi-tier model



17868

The tier layers perform the following functions:

- The resource layer describes external or legacy systems, which include the network of managed devices and the Oracle database. Managed devices are the resources that can be configured, controlled, and monitored by the 5620 SAM. The Oracle database contains the persistent storage for the data model, with data such as device configurations and statistics, as well as information about customer connections and services.
- The integration layer buffers resource-layer entities from the business layer. This layer contains the mediators, which communicate with equipment in the managed network, and the database adapter. The mediator components translate messages from the business layer into the SNMP, FTP, secure FTP, and CLI messages that are sent to the managed network. Messages that are received from the network are processed by the mediator components and passed to the business layer. The integration layer also contains the database adapter that decouples the Oracle database from the business logic. The database adapter code translates business logic requests into JDBC commands, and translates JDBC responses into the Java business model.
- The business layer contains the Java application logic and data model that drive 5620 SAM functionality. The business logic processes input from client requests, managed network traps, and internal server events, and performs the appropriate actions on the managed network, clients, and internal data model. The server data model maintains information about network objects and their relationships. To support the business layer, an application server provides J2EE services.
- The presentation layer buffers the application logic from the client layer. This layer contains several components. The web server receives SOAP/XML messages from OSS clients and passes them to the business layer. The third-party

application server handles EJB method invocations received from the 5620 SAM GUI clients on the network and returns the responses generated by the business-layer logic. The application server also forwards JMS asynchronous messages from the business layer to 5620 SAM clients for event notification.

- The client layer comprises the OSS clients and 5620 SAM GUI clients. The 5620 SAM GUI client installation package contains a Java virtual machine and Java GUI components that send EJB remote method invocations to the 5620 SAM server. The OSS clients send XML/SOAP messages to the 5620 SAM server. The 5620 SAM architecture also supports web portal interfaces.

Server data model

The server data model is the framework for service-level functionality. It represents the physical and logical elements of the network, such as equipment, customers, services, accounting data, and network performance statistics. The model also describes the relationships between these entities, thereby allowing users to perform network operations at the service level or customer level. This ability to associate entities in the network provides enhanced service capabilities and is crucial for managing complex multiservice networks.

The data model representation of the current state of the managed network is stored in the Oracle database. Changes to the model that are triggered from the network include event and data notifications such as network device fault traps or state changes. These updates are applied to the model, stored in the database, and reported to the client interfaces. Changes to the model that are triggered from clients include configuration or provisioning changes. These changes are applied to the model, stored in the database, and deployed to the network when appropriate.

Distributed server architecture

The 5620 SAM server functionality can be distributed across multiple physical platforms in a standalone or redundant 5620 SAM configuration. A main server and one or more auxiliary servers in the same 5620 SAM domain define a 5620 SAM server cluster. A redundant 5620 SAM system has two clusters—one for each main server. The auxiliary servers are members of only the cluster that contains the current primary main server. When the main servers change roles, for example, after a server activity switch, the auxiliary servers leave the current cluster and join the one that contains the new primary main server.

See the 5620 SAM Redundancy chapter of the *5620 SAM User Guide* for information about auxiliary-server roles and behavior in a redundant 5620 SAM system. See the *5620 SAM Planning Guide* for information about auxiliary-server platform requirements and scalability considerations.

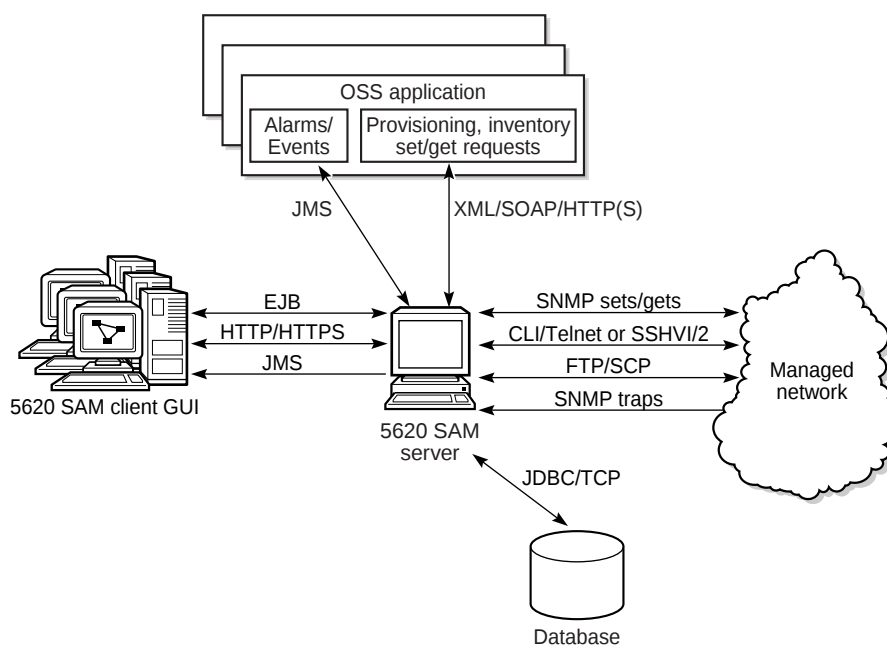
The main server in a cluster is the network-management engine that processes GUI and OSS client requests and monitors the network elements. It also directs the operation of the auxiliary servers and distributes the processing load to them as required. This distributed functionality is invisible to 5620 SAM GUI and OSS clients because they interact only with the main server.

The main server sends new or updated operating information, for example, the 5620 SAM license capacity, redundancy status, and database credentials, to each auxiliary server as the information becomes available. It also sends the current topic name and associated JNDI and HAJNDI information as required.

1.3 Component interfaces

The 5620 SAM component interfaces use industry-standard protocols for communication between servers and the database, managed network devices, and clients, as shown in Figure 1-2.

Figure 1-2 5620 SAM interfaces



17901

Servers and managed devices

5620 SAM main and auxiliary servers send messages to the managed network in the form of SNMP sets and gets, JDBC JMS messages, and FTP or secure FTP (SCP) commands. A 5620 SAM main server also uses CLI commands over Telnet or SSH.

- 5620 SAM servers use SNMP to monitor and manage network performance and to identify network problems. Main servers deploy configuration changes to the managed devices using SNMP. Auxiliary servers poll MIB performance data stored on the managed devices. The managed devices use asynchronous SNMP messages called traps to notify the 5620 SAM main server about device events.
- The command-line interface (CLI) on a managed device is accessible through a 5620 SAM client using Telnet, SSHv1, or SSHv2. A 5620 SAM operator uses CLI commands to modify device configurations and to perform troubleshooting.

functions. An operator with the appropriate user-account privileges can gain access to a device CLI by sending messages to the 5620 SAM server, which serves as an intermediary between the network devices and clients.

- FTP and SCP are transport layer protocols for transferring files between systems. The 5620 SAM uses these protocols for backing up managed device configuration data, collecting accounting statistics from the devices, and downloading software from the main server to devices.
- JMS is a subscription service that allows clients to receive event and alarm messages about the state of the managed network. It runs in a dedicated JVM on a main server.

Main server and clients

Client interfaces provide access to the 5620 SAM main server and to the managed network. Clients send requests to the 5620 SAM main server to view and change data objects in the data model and to perform network operations. The OSS clients use the XML/SOAP protocol over HTTP or HTTPS. The client GUIs use Java session bean invocations. A 5620 SAM main server communicates with clients as follows:

- OSS client software developers create XML requests for processing by the 5620 SAM main server. Schema files provide the XML interface definitions for data objects. The schema files package related domain objects together and describe the attributes and methods of the objects. The JMS interface is also available using XML messaging. See the *5620 SAM-O OSS Interface Developer Guide* for more information about the contents of the schema files and the messages that are sent between OSS clients and a 5620 SAM main server.
- The 5620 SAM GUI clients send requests to the server EJB session beans using Java RMI.
- The 5620 SAM GUI auto-client update functionality uses HTTP or HTTPS for client update communication and file downloads.
- The JMS and the XML publisher service run on the same physical station as a main server, but in a separate JVM. This reduces the stack size for a processing thread and supports multiple simultaneous client connections.
- The 5620 SAM GUI and 5620 SAM-O OSS clients use JMS channels to receive real-time network event information from the server. Clients must register a subscription or durable subscription using object messaging to set up a JMS channel. The received event types include:
 - managed network alarm notifications
 - managed network configuration changes
 - server activity-switch notifications
 - 5620 SAM database connectivity errors

Main server and database

A 5620 SAM main server communicates with a 5620 SAM database using a JDBC session over TCP. JDBC is a Java API for interworking with SQL relational databases.

Main server and auxiliary servers

Each 5620 SAM main server includes a mechanism for sending requests to auxiliary servers. A main-server functional area that uses this mechanism, for example, a statistics-collection scheduler, performs load balancing to equally distribute the requests among the available auxiliary servers. An auxiliary server notifies the main server after it finishes processing a request. If the main server fails to send a request or all available auxiliary servers are unresponsive to a request, the main server raises an alarm, for example, MissedStatsCollection.

5620 SAM and external systems

The 5620 SAM can be integrated with an external network- management system such as the 5620 NM. During 5620 SAM client installation, you can configure navigation from an external system for additional network-monitoring capability.

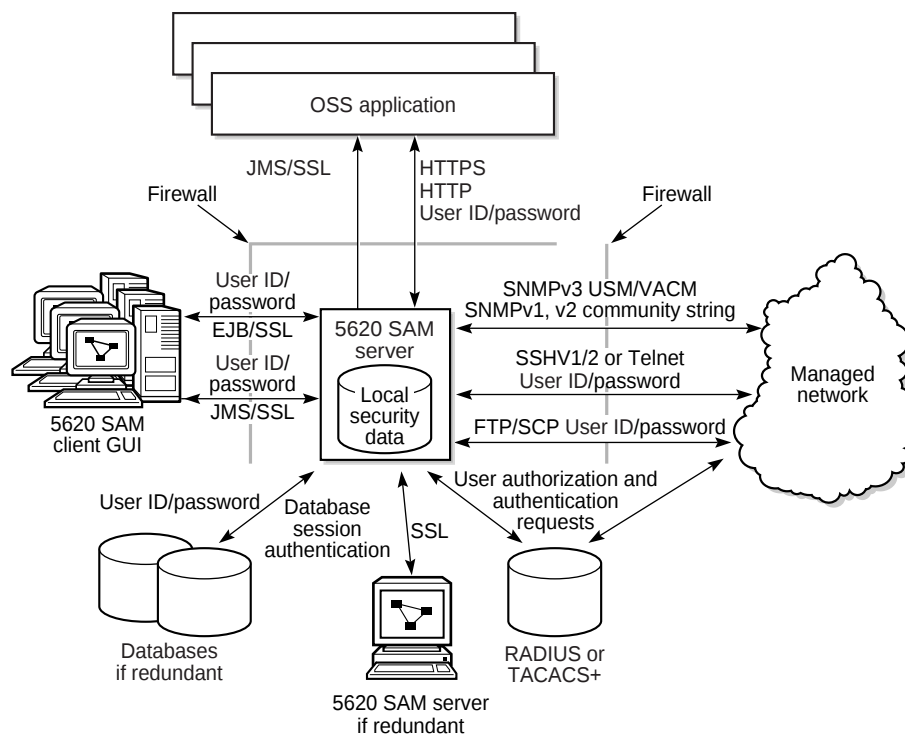
1.4 Security

A distributed system such as the 5620 SAM requires security at the session layer and at other communication layers because messages sent over a network can be intercepted and forged. A GUI or OSS client must provide user identification and a password for access to the 5620 SAM functionality. The session credentials and subsequent messages can be protected in the network using various mechanisms and protocols that include the following:

- HTTPS as the application layer transport mechanism for OSS clients
- Telnet, SSH, SCP and SNMPv3 with USM or VACM at the application layer for communication with the managed network
- SSL at the presentation layer, between a main server and GUI or OSS clients, or between the primary and standby main servers in a redundant configuration
- NAT and IP validation at the network layer, between main servers and auxiliary servers, databases, or GUI or OSS clients

Figure 1-3 shows the 5620 SAM components and the available security mechanisms.

Figure 1-3 5620 SAM security



18083

Session management

Effective session management requires authentication, authorization, and accounting (AAA) functionality. Authentication is the verification of a user identification and password. Authorization is the assignment of different levels of access permissions to users. Accounting is the recording of user actions. A 5620 SAM operator can configure AAA functionality using the local security capability of the 5620 SAM server, a third-party authentication server, or a combination of local and third-party mechanisms.

- Local authentication on the 5620 SAM server is provided with a local database of users and a local security scheme to verify logon attempts and assign permission levels for command execution.
- Supported third-party authentication servers are RADIUS and TACACS+. These products run on their own platforms, with their own user lists and administration processes.

5620 SAM user accounts consist of a user name, password, and an associated user group and scope of command. User groups are used to assign and control user authorization levels, and to control the extent of access to such entities as customers, services, or faults. The system administrator can also limit the type of user access per managed device; for example, by allowing FTP access but denying console, Telnet, or SNMP access.

Client sessions

All client sessions have username and password protection.

- The 5620 SAM client GUI EJB sessions are protected by the username and password for the session.
- Each OSS client XML/SOAP message is individually authenticated using cached information from an authorization server.
- JMS messages are protected by the user name and password for the JMS connection.

Database sessions

The database is accessible through a connection from the server, which is protected by a user ID and password. When a database update is completed, an entry in the client activity log saves the client name and the request performed to track user actions on the database workstation.

Secure communication between a 5620 SAM server and an Oracle database is available through network security mechanisms such as NAT and IP-address validation. You can configure network security for the 5620 SAM during the installation of a 5620 SAM system.

Managed device sessions

The 5620 SAM server runs CLI, FTP, or secure FTP (SCP) commands on managed devices. Clients can also run these commands by issuing requests to the server. A managed device uses the local security database or a third-party service such as RADIUS or TACACS+ to perform AAA security functions.

SNMPv3 message authentication and authorization is handled by the USM and VACM mechanisms to define users and user authorization permissions. Older SNMP versions are authenticated with community string identifiers. Every SNMP message is individually authenticated.

Network transport security

Transport layer security is available to the network protocols that carry messages between programs running on different platforms.

Main server and clients

Network communication between the 5620 SAM server and clients is carried out using XML/SOAP, EJB, or JMS messages.

- The OSS clients have two options for message security. When HTTPS is used to transport XML/SOAP messages, messages are protected by SSL functionality. The less-secure HTTP can also be used.
- The Java GUI clients use the EJB interface, which is protected by an SSL connection.
- Both OSS and GUI clients use JMS, which is protected by SSL.
- In a redundant configuration, the secondary 5620 SAM server acts as a client of the primary server, which is protected by SSL.

Servers and managed devices

Messages are sent by a managed device to a 5620 SAM main or auxiliary server using SNMP, FTP, or SCP. When SNMPv3 is used, then SHA or MD5 authentication values are placed in messages and checked against an encryption key shared by the server and the managed device.

SSH provides the security for a CLI session between a 5620 SAM GUI client and a managed device.

RSA encryption is available for communication between auxiliary servers and managed devices. Contact Alcatel-Lucent support for more information about RSA encryption for auxiliary servers.

Firewall support

The 5620 SAM supports firewalls on all the server interfaces, that is, between the main server and auxiliary servers or clients, and between a main or auxiliary server and the managed network. See the *5620 SAM Planning Guide* for firewall and reserved port information.

1.5 Fault tolerance

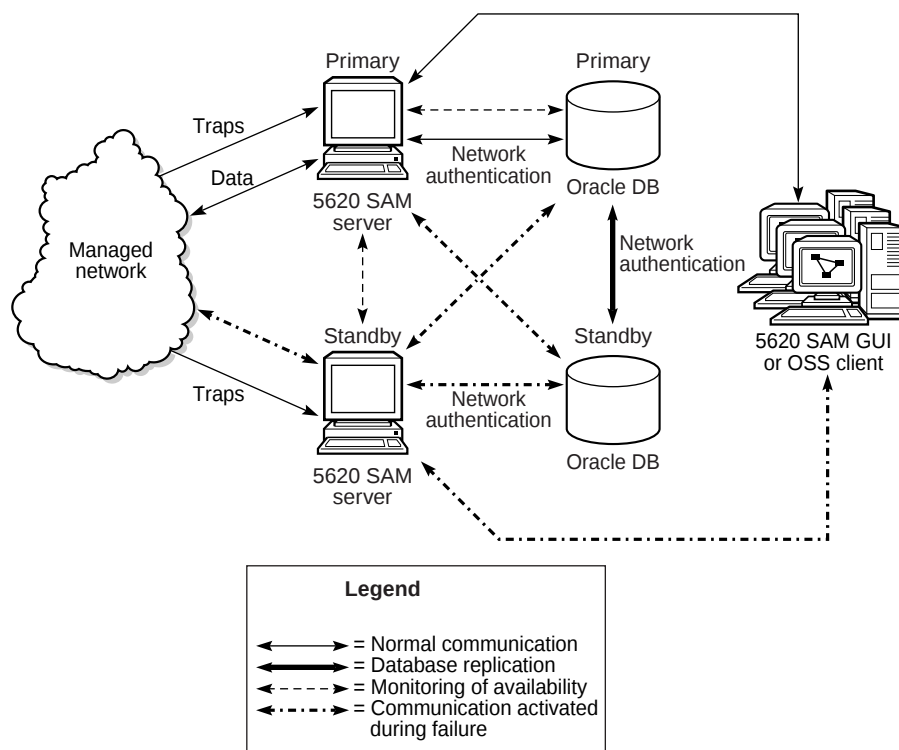
Fault tolerance provides the reliability that customers expect by maintaining system availability in the event of a system component failure. 5620 SAM fault tolerance includes high availability through component redundancy. Deploying the 5620 SAM hardware and software components in a redundant configuration ensures that there is no single point of failure within the 5620 SAM system.

Redundant physical network interfaces and points of network entry ensure that there is no single point of failure between the 5620 SAM system and the managed network. Redundant network paths, for example, in-band and out-of-band management, can help to prevent the isolation of a 5620 SAM server from the network in the event of a device failure in the managed network.

Main server and database redundancy

A redundant 5620 SAM system consists of a primary server and an associated primary database that actively manage the network, and a second server and database pair in standby mode. A 5620 SAM server and database pair can be collocated on one station or run on separate stations. Figure 1-4 shows a fully distributed, redundant 5620 SAM configuration.

Figure 1-4 5620 SAM redundancy



17903

Secure communication between a 5620 SAM server and an Oracle database is available through network security mechanisms such as NAT and IP-address validation. You can configure network security for the 5620 SAM during 5620 SAM system installation.

See the *5620 SAM User Guide* for more information about 5620 SAM redundancy.

Main server redundancy

5620 SAM main server redundancy is achieved through clustering technology provided by a JBOSS Java application server on each main server. The primary and standby main servers regularly poll each other to monitor availability. The 5620 SAM server software state is held only on the primary server. Traps from the managed network are always sent to both primary and standby servers to avoid delays if an activity switch occurs.

If the primary server loses visibility of the standby server, it notifies the GUI clients. If the standby server loses visibility of the primary server, the standby server attempts to become the primary server by connecting to the primary database. The newly active server obtains its current state from the database.

Database redundancy

5620 SAM database redundancy is based on Oracle Data Guard Replication, which keeps the standby database synchronized with data changes that take place on the primary database. The supported fault-recovery operations are database switchover and database failover. A switchover is performed between two functioning databases to switch roles between primary and standby databases. A failover forces the standby database to become the primary database in the event of primary database failure or unavailability.

The primary 5620 SAM main server polls both databases to check for their availability. If the primary or standby database is unavailable, the server notifies the 5620 SAM GUI clients. If both 5620 SAM servers lose contact with the primary database, a failover occurs and the standby database becomes the new primary database.

Network session authentication is provided using the SYS user password that is configured during 5620 SAM system installation.

Auxiliary servers and 5620 SAM redundancy

Auxiliary servers are passively redundant. They do not cause or initiate main server or database redundancy activities, but if a Preferred auxiliary server ceases to respond to requests from the primary main server and a Reserved auxiliary server is available, the main server directs the current and subsequent requests to the Reserved auxiliary server until the Preferred auxiliary server is again available.

An auxiliary server communicates only with the server and database that are currently designated primary. After a 5620 SAM redundancy activity, for example, a database failover, the primary main server directs the auxiliary servers to stop communicating with the former primary component and instead communicate with the new primary component.

See the *5620 SAM User Guide* for more information about auxiliary servers and redundancy.

1.6 Network management capabilities

The 5620 SAM network management system provides flexible network access that allows users to interact with the network on a per-service or per-customer basis, or at the level of individual devices. The ability of the 5620 SAM to link customers, services, equipment, and faults provides the ability to efficiently manage a complex network by simplifying routine operations and allowing bulk provisioning.

The 5620 SAM creates a data model of the network that includes the relationships between customers, services, and equipment. The main and auxiliary servers collect data from managed devices and collate the data for billing, performance monitoring, troubleshooting, and inventory and alarm reporting at the service or customer level. The main server deploys user commands to the network and performs autonomous functions such as device discovery and backups.

5620 SAM network-management functional areas

The 5620 SAM features the following capabilities:

- alarm correlation up to the service level
- service and routing provisioning using policies and profiles to reduce the repetition of effort
- inventory reporting at the equipment, service, and customer levels using filtered views that can be saved as report files
- network performance and accounting data collection on a per-service or per-port basis using a flat-rate, destination, or usage schema
- troubleshooting at the service level, which includes viewing the associations between services and entities such as customers, equipment, and transport tunnels
- an XML interface that provides access to 5620 SAM functionality from other network-management systems or portals

Service management

The service management capabilities of the 5620 SAM allow network operations staff to provision VLL, VPLS, IES, VPRN, or VLAN services for customers. These service networks can then be tracked for performance monitoring, billing, inventory, reporting, and alarms. You can track the managed network data from SNMP traps, billing and traffic analysis data, and SNMP MIB performance data. The data is rolled up and correlated using the server data model and server business logic.

The 5620 SAM allows the provisioning of service mirrors to monitor service traffic for troubleshooting or official surveillance purposes.

Billing

The 5620 SAM collects accounting statistics stored on managed devices for the creation of billing records and for traffic-analysis purposes. The statistics are transferred to the 5620 SAM servers using FTP or SCP.

Equipment management

Physical equipment is:

- discovered and the 5620 SAM database is initially populated
- resynchronized with the 5620 SAM database and the content of the database is matched with the content of the physical device database
- configured when clients send requests to add new equipment or change existing equipment

The server makes the appropriate changes to the data model and deploys the updates on the relevant nodes. For example, when a card is added to a node, the server data model is updated, and the card configuration commands are sent to the node.

Network configuration is supported for MPLS, LSP, and service tunnels, as well as routing protocols such as RIP, BGP, and ISIS. These configurations are requested by clients and deployed to the network. New nodes can be discovered by a user request or automatically through server polls. When a new node is discovered, it is added to the data model and set to a managed state.

Performance management

The 5620 SAM provides the ability to monitor services and resources using performance statistics, diagnostic tools and data validation; it raises a related alarm as appropriate. To protect against data loss, the 5620 SAM can perform scheduled backups of the 5620 SAM database and the managed-device configurations.

- The 5620 SAM collects performance statistics through polls of the managed devices. Managed devices use SNMP to upload network performance statistics data in the local MIBs to the 5620 SAM.
- The 5620 SAM diagnostic tools include MAC ping, VCCV ping for VLL services, DNS ping for name resolution, LSP ping and traceroute, and VPRN ping. Performing service and service-transport connectivity tests during service creation can ensure correct functionality at service activation time. Ping tests against management IP addresses indicate managed-device availability.
- The 5620 SAM compares the configuration information on managed devices with the information in the database to ensure information synchronization.
- The 5620 SAM can perform a scheduled backup of the 5620 SAM database and the managed device configuration files to a secure location.

Fault management

Fault management occurs in response to the SNMP traps sent by managed devices to the 5620 SAM. The 5620 SAM main server converts a trap to a status update and raises an alarm against the entity when appropriate. 5620 SAM GUI clients use visual and auditory signals to alert the operator to the arrival of an alarm.

Managed devices send SNMP traps to indicate a number of conditions that include configuration or operational-state changes, security breach attempts, and equipment faults. The traps are passed to clients immediately if they have registered for a JMS event channel, or later when the client polls the server.

1.7 Standards compliance

Table 1-1 describes 5620 SAM standards compliance.

Table 1-1 5620 SAM standards compliance

Standard	Description
ITU-T X.721	SMI
ITU-T X.734	Event report management function
M.3100/3120	Equipment and connection models
TMF 509/613	Network connectivity model
MTOSI	Compliance of generic network objects, inventory retrieval, and JMS over XML
RFC 1213	SNMPv1
RFC 1738	Uniform Resource Locators (URL)
RFC 3416	SNMPv2c
RFC 3411-3415	SNMPv3
RFC 2138	RADIUS client 2618
draft-grant-tacacs-02.txt	TACACS+ client
XML	W3C XML 1.0
XML	W3C Namespaces in XML
XML	W3C XML schemas
SOAP	W3C SOAP 1.2
draft-ylonen-ssh-protocol-00.txt	SSH
ISO 8601	Calendar date
RFC 0959	FTP
J2EE	JMS
EJB 2.3	J2EE Enterprise Java Session Bean

Alcatel-Lucent considers the following standards in the design of the 5620 SAM GUI:

- Sun Microsystems, *Java Look and Feel Design Guidelines*, Addison-Wesley Publishing Company, Reading, Massachusetts 1999.
- ANSI T1.232-1996, *Operations, Administration, and Provisioning (OAM&P)- G Interface Specifications for Use with the Telecommunications Management Network (TMN)*.
- Telcordia (Bell Core) GR-2914-CORE Sept. 98, *Human Factors Requirements for Equipment to Improve Network Integrity*.
- Telcordia (Bell Core) GR-826-CORE, June 1994, Issue 1, Section 10.2 of OTGR, *User Interface Generic Requirements for Supporting Network Element Operations*.
- ITU-T Recommendation Z.361 (02/99), *Design guidelines for Human- Computer Interfaces (HCI) for the management of telecommunications networks*.
- ETSI EG 201 204 v1.1.1 (1997-05), *Human Factors (HF); User Interface design principles for the Telecommunications Management Network (TMN) applicable to the “G” Interface*.

Glossary

Numerics

5620 NM	5620 Network Manager The 5620 NM provides advanced management of large, complex LAN/WAN networks, including hybrid circuit-switched, IP/MPLS, ATM, frame relay, and X.25 networks. The GUI operates on a Sun workstation. It can be used to configure databases, monitor network operation in real time, set up and manage paths, and perform diagnostics to isolate and manage problems on the network. With the addition of optional software modules, the 5620 NM can perform advanced management functions such as managing multivendor equipment, interfacing with UMS, and partitioning networks.
5620 SAM	5620 Service Aware Manager The 5620 SAM is the network manager portfolio of modules for the 7750 SR, 7710 SR, 7450 ESS, 7250 SAS, and Telco devices.
5620 SAM auxiliary server	In a 5620 SAM system that is deployed using distributed server architecture, a 5620 SAM server instance on a dedicated station that accepts processing requests from, and is directed by, a 5620 SAM main server. A main server and one or more auxiliary servers that are in communication are collectively called a 5620 SAM server cluster.
5620 SAM client	The 5620 SAM client provides a GUI to configure IP network elements.
5620 SAM database	The 5620 SAM database stores network data-model objects and network configuration information.

5620 SAM main server	A server instance in the 5620 SAM distributed server architecture that directs one or more 5620 SAM auxiliary servers and interacts with 5620 SAM clients. The term is meaningful only in the context of a distributed 5620 SAM server deployment; the term 5620 SAM server applies to a single server instance in a non-distributed 5620 SAM deployment. A main server and one or more auxiliary servers that are in communication are collectively called a 5620 SAM server cluster.
5620 SAM server	The 5620 SAM server mediates between the 5620 SAM database, the 5620 SAM client, and the network. A 5620 SAM server may be a single server instance, or, in a distributed server architecture, a server cluster that consists of one main server and one or more auxiliary servers.
5620 SAM server cluster	A logical grouping in a distributed 5620 SAM server configuration that consists of a 5620 SAM main server and the 5620 SAM auxiliary servers in communication with it.
5750 SSC	5750 Subscriber Services Controller This product allows carriers to manage 5620 SAM subscriber services, and also allows customers to configure their own 5620 SAM services from Web portals.
7450 ESS	7450 Ethernet Service Switch The 7450 ESS is a router that provides scalable, high-speed Ethernet private data services with SLAs.
7710 SR	7710 Service Router The 7710 SR is a 10 Gbyte version of the 7750 SR that provides granular lower-speed private data services with SLAs.
7750 SR	7750 Service Router The 7750 SR is a router that provides scalable, high-speed private data services with SLAs.
A	
API	application programming interface
Application Server	Software product that provides J2EE services for Java applications, such as JMS or transactions support. It may also include clustering technology to allow multiple Java virtual machines to communicate over a network.
ASN.1	Abstract Syntax Notation One
auxiliary server	See 5620 SAM auxiliary server .

C**CLI**

command line interface

A system console interface for performing operations on a device.

E**EJB**

Enterprise Java beans

Used to describe a session bean, which is a Java object tied into system services to provide session management functionality. EJB technology is the architecture on the server side for the Java 2 Platform, Enterprise Edition.

F**FTP**

file transfer protocol

FTP is the Internet standard client-server protocol for transferring files from one computer to another. FTP generally runs over TCP or UDP.

G**GUI**

graphical user interface

H**HTML**

HyperText Markup Language

Language for writing hypertext documents, often for use in a web environment.

HTTP

hypertext transfer protocol

HTTP is the basic protocol of the World Wide Web, defining the protocol between browsers and servers.

HTTPS

hypertext transfer protocol secure

HTTPS is HTTP over SSL, which uses a public-and-private key encryption system, including the use of a digital certificate for secure transfer of web messages.

I

IES	internet enhanced service A routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic.
IETF	internet engineering task force The organization that provides coordination of standards and specifications developed for IP network and related protocols.

J

J2EE	Java 2 Enterprise Edition A set of services, APIs, and protocols that provide the functionality to develop multi-tiered, web-based application components. J2EE is overseen by a partnership of enterprise software and computer platform vendors, and is available on a wide range of platforms.
Java	Java is an object-oriented programming language developed by Sun Microsystems that supports interaction between remote objects. Computer programs written in Java can run on any platform that is running a Java Virtual Machine.
JDBC	Java database connectivity A Java API for exchanging data with SQL relational databases.
JMS	Java message service An API for reliable asynchronous communication among components in a distributed computing environment.

L

Linux	An open-source, UNIX-like operating system.
--------------	---

M

main server	See 5620 SAM main server .
MD5	A one-way hash encryption method
MIB	management information base

MTOSI multi-technology operations systems interface

A TMF team creating new standards for OSSs to simplify integration between different vendors' systems by using a common open interface.

A TMF standard defining

multi-tier model Logical partitioning of software products to enable distributed implementations and modular deployments. Logical partitioning can be from three layers (user interface, application server or middleware, database server) to five or more layers. One model uses the client, presentation, business, integration, and resource layers to define software components.

O

Oracle Advanced Security A security option for the Oracle database product that provides security features to protect enterprise networks and securely extend corporate networks to the Internet. Oracle Advanced Security combines message encryption, database encryption, strong authentication, and authorization to address customer privacy and compliance requirements.

OSS operational support system

A network management system that supports a specific management function, such as alarm surveillance and provisioning, in a service provider network.

P

ping packet internet groper

An ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

R

RADIUS remote authentication dial in user service

An authentication, authorization and accounting (AAA) protocol for applications that allows remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It allows a company to set up a policy that can be applied at a single administered network point.

RMI remote method invocation

A Java API allowing Java objects to make remote procedure calls to other Java objects in a network.

S

SCP secure copy protocol, also known as secure FTP. See “FTP”.

SMI structure of management information

A description of the common structure and identification scheme for the definition of information used in managing TCP/IP-based internets. Formal descriptions of the structure are given using ASN.1. SMI is defined in RFC 1155.

SNMP simple network management protocol

A protocol used for the transport of network management information between a network manager and a network element. SNMP is the most commonly-used standard for most interworking devices. SNMPv3 is the most recent and secure version.

SNMP trap An unsolicited notification that indicates that the SNMP agent on the node has detected a node event, and that the network management domain should be aware of the event. SNMP trap information typically includes alarm and status information, and standard SNMP messages.

SOAP simple object access protocol

A lightweight protocol that is commonly used to send XML messages over the Internet. When SOAP is bound with HTTPS, a secure message containing XML can be sent to web servers.

Solaris The name for the UNIX operating system variant developed by Sun Microsystems.

SQL structured query language

A specialized language for accessing relational databases.

SSH secure shell

This protocol is used to support secure remote login. SSH runs over TCP, authenticating and then encrypting a session. It is a secure alternative to Telnet but can also be used for FTP, SNMP, and remote execution of programs.

SSL secure socket layer

A protocol that provides endpoint authentication and communications privacy over the Internet using cryptography. SSL is layered beneath application protocols such as HTTP, Telnet, and FTP, and is layered above TCP. It can add security to any protocol that uses TCP.

T

TACACS+ A remote user authentication, authorization, and accounting protocol.

TCP transmission control protocol

A transport layer protocol used to establish connections and send data between computers over the Internet. It runs on top of IP.

Telnet The Internet-standard TCP/IP protocol for remote login service. It allows a user at one site to interact with a remote system at another site.

TMF telemanagement forum

A non-profit global organization that provides leadership, strategic guidance and practical solutions to improve the management and operation of information and communications services.

U

UI user interface

USM user-based security model

V

VACM view-based access control model

A model of the access control subsystem of an SNMP engine, which defines a set of services that an application can use for checking access rights.

VLL virtual leased line

A type of VPN where IP is transported in a point-to-point manner.

VPLS virtual private LAN service

A type of point-to-multipoint VPN in which a number of sites are connected in a single bridged domain (Layer 2) over an IP/MPLS network.

VPN virtual private network

VPRN virtual private routed network

A point-to-multipoint VPN with Layer 3 interfaces. Also known as IP-VPN.

W

web services Web services are a way of developing functionality and putting it out on the web so other programs can access it through a well-defined interface. The meta-language XML and the protocol SOAP allow the definition and transmission of messages between software components running on heterogeneous platforms. This allows development teams to independently build components that run as distributed, independent implementations, linked only by their XML interface.

X

XML

extensible markup language

A meta-language that can be used both to define a language syntax and to encode messages in that language. It is commonly used to send platform-independent messages over the Internet, for example, between clients and servers.

Index

Numbers

5620 SAM

- architecture, 1-2
- components, 1-3
- integration with external systems, 1-8
- interfaces, 1-6, 1-8
- multi-tier model, 1-3
- network management, 1-14
- redundancy, 1-12
- security, 1-9
- standards compliance, 1-16

5620 SAM clients

- and server, 1-7
- interfaces, 1-7
- network transport security, 1-11
- session security, 1-10

5620 SAM database

- and main server, 1-7
- interfaces, 1-7
- redundancy, 1-12
- session security, 1-10

5620 SAM interfaces, 1-6

- 5620 SAM and external systems, 1-8
- firewalls, 1-11
- main server and auxiliary servers, 1-8
- main server and database, 1-7
- server and clients, 1-7
- server and managed devices, 1-6

5620 SAM server

- and clients, 1-7
- and managed devices, 1-6
- data model, 1-5
- features, 1-14
- interfaces, 1-6
- network transport security, 1-11
- redundancy, 1-12

A

architecture, 1-2

- availability, 1-12
- components, 1-3
- interfaces, 1-6
- multi-tier model, 1-2
- network management, 1-14
- open standards, 1-2
- security, 1-9
- server data model, 1-5
- session management, 1-10
- web service model, 1-2

auxiliary servers, 1-8

- availability, 1-12

B

- billing, 1-14

C — web service model

C

clients; *See* [5620 SAM clients](#)
components, [1-3](#)

D

database; *See* [5620 SAM database](#)
devices; *See* [managed devices](#)
documentation, [x](#)

E

equipment management, [1-15](#)
external systems, [1-8](#)

F

fault management, [1-15](#)
firewalls, [1-11](#)

I

interfaces; *See* [5620 SAM interfaces](#)

M

managed devices
 [interfaces, 1-6](#)
 [network transport security, 1-11](#)
 [session security, 1-10](#)
models
 [multi-tier, 1-3](#)
 [server data, 1-5](#)
 [web service, 1-2](#)
[multi-tier model, 1-2](#)
 [tier layers, 1-3](#)

N

[network management, 1-14](#)
 [5620 SAM server features, 1-14](#)
 [billing, 1-14](#)
 [equipment, 1-15](#)
 [faults, 1-15](#)
 [performance, 1-15](#)
 [services, 1-14](#)
 [transport security, 1-11](#)

[network transport security, 1-11](#)
 [server and clients, 1-11](#)
 [server and managed devices, 1-11](#)

O

[open standards, 1-2](#)

P

[performance management, 1-15](#)

R

[redundancy, 1-12](#)

S

[security, 1-9](#)
 [firewalls, 1-11](#)
 [network transport, 1-11](#)
 [server and clients, 1-11](#)
 [server and managed devices, 1-11](#)
 [session management, 1-10](#)
server; *See* [5620 SAM server](#)
[service management, 1-14](#)
[session management, 1-10](#)
[standards compliance, 1-16](#)

U

[user documentation, x](#)

W

[web service model, 1-2](#)

Customer documentation and product support



Customer documentation

<http://www.alcatel-lucent.com/osds>

Product manuals and documentation updates are available through the Alcatel-Lucent Support Documentation and Software Download service 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://www.alcatel-lucent.com/support>



Customer documentation feedback

documentation.feedback@alcatel-lucent.com

