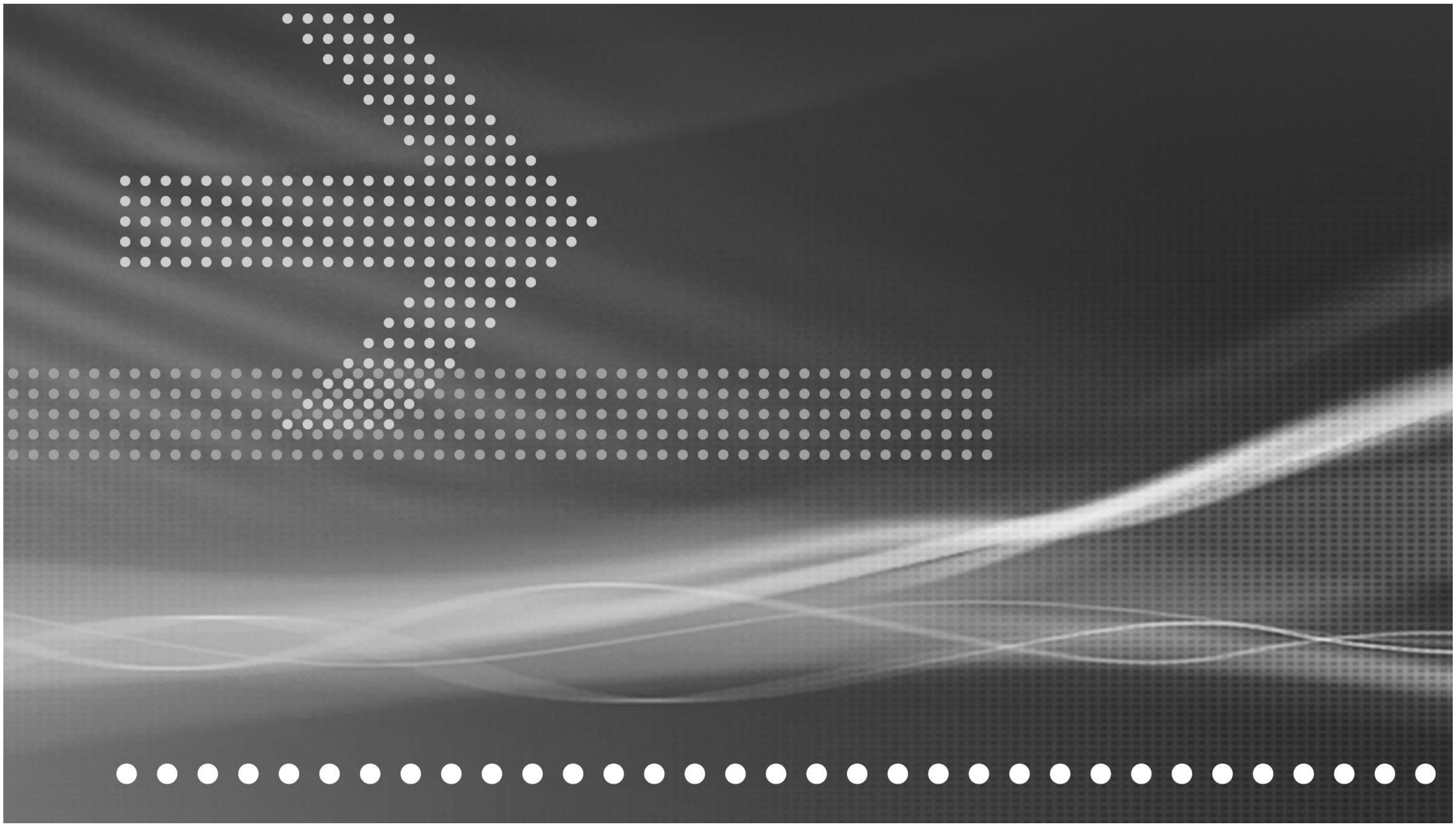


Alcatel-Lucent

IP MULTIMEDIA SUBSYSTEM RELEASE 07.05.01

SOLUTION EXTERNAL RELEASE NOTES

275-100-
004R07.05.01
SEPTEMBER 2009
ISSUE 1.0

Legal Notice

Contents

About this document

Purpose

The purpose of this document is to provide a general overview of the IP Multimedia Subsystem (IMS) Release 07.05.01, including a list of the network element load versions, IMS network level test results, and known issues to assist service providers with field deployments of IMS Release 07.05.01.

Reason for revision

This is the first issue of the IMS Release 07.05.01 Release Notes.

Intended audience

The intended audience for this document includes all personnel who need information about the IMS 07.05.01 release, its functions, and network elements.

This document can be used by the following audiences:

- Planning and design personnel
- Maintenance personnel
- Management personnel
- System installation and integration personnel

Supported systems

See Chapter 7, System Requirements, for information on systems supported in Release 07.05.01.

Conventions used

There are no special typographical conventions used in this document.

Technical support

For technical support, contact your local Alcatel-Lucent customer support team. See the Alcatel-Lucent Support web site (http://alcatel-lucent.com/support/) for contact information.

How to order

This document is available on the Online Customer Support Site (OLCS). To order this document and other Alcatel-Lucent documents, contact your local sales representative or use the Online Customer Support Site (OLCS) web site (https://support.alcatel-lucent.com).

How to comment

To comment on this document, go to the Online Comment Form (http://infodoc.alcatel-lucent.com/comments/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

1 Release components

Overview

Purpose

This chapter describes the loads that comprise Release 07.05.01 and the documentation deliverables included in this release.

Software deliverables

Table 1-1 lists the loads that comprise IMS Release 07.05.01. Changes are shown in bold text.

Table 1-1 Software release identification

Network Element/Application	Load Name in IMS 07.05.00	Load Name in IMS 07.05.01	Load Changed Since IMS 07.05.00?
1300 Cross Management Center (XMC)	R6.2.2.5 Then patch to R6.2.2-P01 Then patch to R6.2.2-N08	R6.2.2.5 Then patch to R6.2.2-P01 Then patch to R6.2.2-N08	No
1310 Operations and Maintenance Center – Plexview (OMC-P)	OMC-P_13_02_00_01	OMC-P_13_02_00_01	No
1440 Unified System Data Server (USDS) (includes MAS/AHE)	USDS: hlr7.3n04.01 MAS: ltmasr27 (R27SU2) – b0102 MAS: ltmasr27 (R27SU2) – 0201 MAS: ltmasr27 (R27SU2) – p0210	USDS: hlr7.3n04.01 MAS: ltmasr27 (R27SU2) – b0102 MAS: ltmasr27 (R27SU2) – 0201 MAS: ltmasr27 (R27SU2) – p0210	No
5410 Presence Server (PS) **5410 SML Document Management Server (XDMS)**	5.0 SP1.1 Hp	**5.0 SP1.2 Hp**	**Yes**
5420 Converged Telephony Server (CTS)	R17.21.00.00 Then patch to R17.21.01.00 Then patch to R17.21.01.01	R17.21.00.00 Then patch to R17.21.01.00 Then patch to R17.21.01.01	No
5420 Voice Call Continuity(VCC) server	N/A	**VCC V8.0.2R21** **JP 1.3.6**	**New**
5440 IMS-PC Client	5440_PCC_r4.0.0_v2315 _nonPCM	5440_PCC_r4.0.0_v2315 _nonPCM	No
5450 IP Session Control (ISC)/ IP Resource Controller (IRC)	R17.21.00.00 Then patch to R17.21.01.00 Then patch to R17.21.01.01	R17.21.00.00 Then patch to R17.21.01.00 Then patch to R17.21.01.01	No
5900 Media Resource Function (MRF)	MRF6.3.4.1	MRF6.3.4.1	No

Network Element/Application	Load Name in IMS 07.05.00	Load Name in IMS 07.05.01	Load Changed Since IMS 07.05.00?
7510 Media Gateway (MGW)	R31N_05_06_2009_M1050609 (R3.1 SP2 CI) A7510_R31N_07_05_2009_B06 (7510 MGW R3.1SP2)	R31N_05_06_2009_M1050609 (R3.1 SP2 CI) A7510_R31N_07_05_2009_B06 (7510 MGW R3.1SP2)	No
8615 Instant enhanced Charging Collection Function (IeCCF)	N440 Hardware: IeCCF R26SU8 and hotslide0106 MAS_ltmasr26-p0814	N440 Hardware: IeCCF R26SU8 and hotslide0106 MAS_ltmasr26-p0814	No
Acme Packet Session Director (4250)	C5.1.1p23	**C5.1.1p29**	**Yes**
Fortinet Fortigate Firewall	v3.0.MR5.8108	**v3.0.MR5.8133**	**Yes**
VitalQIP	VitalQIP R7.1 PR2 (patch B158)	VitalQIP R7.1 PR2 (patch B158)	No

How to obtain software

Please contact your Alcatel-Lucent representative to obtain software.

Document deliverables

For Release 07.05.01, this document is the only solution document that is being published. The *IMS Solution Technical Description*, *Growth, Ports and Protocols, System Parameters,* and *Interface Changes Specifications* documents are not being reissued for this release. See Appendix A of the *Release Notes* for impacted sections of these documents.

For all other solution documents, please use the latest version (Release 07.04.00).

See the next section, “To obtain documentation”, for detailed information on how to obtain IMS Solution documentation.

To obtain documentation

IMS Solution and product documentation is available to IMS Solution customers through OnLine Customer Support (OLCS).

To navigate OLCS, do the following:

1. Go to (https://support.lucent.com/portal/productIndexByCat.do).
2. After a successful login, select **Services Collaboration** from the list on the left side of the page.
3. Select **IMS Solutions** from the list in the middle of the page.

From here, you can access the documentation through either the **IMS Solution Level Documentation** section or by selecting a network element from the **Links to network elements in the IMS Solution** section.

2 New features

Overview

Purpose

This chapter lists the features included in Release 07.05.01.

New features

The following features are included in this release:

Table 2-1 Features released in 07.05.01

Feature Number	Feature Title
13987.30	Presence Content XDMS
13987.31	RCS 1.0 support by PS/XDMS 5.0
33333.231	E2E testing VCC 8.0.2 for IMS 7.5
33333.235	CPRS testing of VCC 8.0.2 with IMS 7.5
33333.243	Test of NNI interface for XDMS 5.0 in IMS 8.2
33333.255	RCS 1.0 Testing of Tri-Op Functions
33333.259	AKA/Ipsec testing with 1440 USDS in IMS 7.5
33333.264	E2E testing of 7510 in bearer path for Video Sessions in IMS 7.5
33333.302	IMS 7.5 O&M End to End Testing

Functionality

See the specific NE documentation for configuration information.

Enhancements

There are no non-feature enhancements in this release.

3 Test results

Overview

Purpose

This chapter provides information on test execution and pass rates.

Test results/exit criteria

The following table shows the results of the IMS 07.05.01 test program. See Table 6-1 for exceptions.

Table 3-1 NLT test results

Solution	Progress Rate	Quality (Pass Rate)	Exit Criteria Status (Reached/Not Reached)
RCS Feature test on IMS 07.05.01	100%	100%	Reached
VCC Feature test on IMS 07.05.01	100%	100%	Reached
VCC CPRS test on IMS 07.05.01	100%	97.5%	Reached
total	100%	99.1%	Reached

4 Changes to fault management, ports, protocols, and parameters

Overview

Purpose

This chapter describes fault management changes (interfaces, alarms, and messages), port and protocol, and system parameter changes in this release.

Interface changes

Changes to Northbound Interfaces

No northbound interface changes have been reported for this release.

Changes to Southbound Interfaces

Please consult the NE-specific documentation for southbound interface changes in this release.

Alarm changes

No alarm changes have been reported for this release.

Message changes

No message changes have been reported for this release.

Port changes

No port changes have been reported for this release..

Protocol changes

No protocol changes have been reported for this release..

System parameter changes

No system parameter changes have been reported for this release.

5 Resolved issues

Overview

Purpose

This chapter describes customer-reported ARs and NLT-reported problems resolved in this release.

Resolved issues

This section lists any resolved issues that were previously reported as *Known Issues* in Chapter 6.

Table 5-1 lists the severity 1 and 2 issues that were resolved in the loads that are part of this release.

Table 5-1 NLT-Reported Severity 1 and 2 Open Issues - Resolved

IMR	NE to Lead	Resolve Rls	Fixed in Load	Current Status	Solution(s)	Exception Description	Impact Statement / Workaround
889308	Fortinet FW	IMS 07.05.01	MR5. 8133	Fixed	ECS / RCS	Fortinet blocks CANCEL SIP message when P-CSCF sends it after 3 minutes	Service Impacted: File transfer with no answer of the receiver: After 3 minutes without accepting the file transfer, the call is cancelled by the network (ISC) but Fortinet has already released the context so Cancel is not sent to the users. Impact: Caller has to cancel manually the transfer request. After the 3 minutes, if the receiver finally accepts the call, file transfer will never happen.
890668	PS/XDMS	IMS 07.05.01	5.0 SP1.2	Fixed	ECS / RCS	Revoke a contact doesn't work in NNI configuration	Service Impacted: Revoking a user from its contact list when this user is in another IMS network (If user A revokes the Presence Relationship with user B, both users shall no longer receive any more updates of their Presence Information for a certain period of time specified by User A). Consequence: User A is able to revoke User B however User A still appears offline in User B's address book Validated OK with private patch.

6 Known issues

Overview

Purpose

This chapter describes NLT-reported issues that remain open in Release 07.05.01.

Known issues and workarounds

As of August 2009, no customer-reported ARs have been opened against this release.

Table 6-1 lists the severity 2 issues that were not resolved in the network element loads that are part of this release.

Table 6-1 NLT-reported severity 2 open issues

IMR	NE to Lead	Resolve Rls	Fixed in Load	Current Status	Solution(s)	Exception Description	Impact Statement / Workaround
890346	VCC	IMS 07.05.02	JP1.3.7	On Target	ECS/VCC	When a non-pilot board is unlocked, there are traffic errors.	Service Impacted: VCC switchover Impact: traffic degraded during 2 min. after unlock. Private already verified; official delivery on JP1.3.7.
892173	VCC	IMS 07.05.02	JP1.3.7	On Target	ECS/VCC	When upgrading OAS 5400. MAS snmp configuration is lost.	Service Impacted: VCC Switch-over Impact: Loss of MAS alarms after platform upgrade, but so far, there is no traffic during platform upgrade.

7 System requirements

Overview

Purpose

This chapter describes IMS GUI Java dependencies and compatibility restrictions.

Software requirements

IMS GUIs JAVA Dependency

Table 7-1 shows IMS GUIs with Java installation dependencies (listed in order of installation sequence).

Table 7-1 IMS GUIs with Java installation dependencies

LCP MI GUI	Java installed per link provided during initial start of MI GUI (Java 1.5.0_06)
XMC GUI	Java installed per link provided during initial start of MI GUI (Java 1.5.0_15)

The following NE GUIs do not have Java dependencies: FS GUI (5420 CTS, 5450 ISC), 1310 OMC-P (Plexview), 5900 MRF, 5420 PCM Platform.

SUN Operating System Patch Level for Non-Integrated Components

Table 7-2 shows the SUN OS patch level for non-integrated components.

Table 7-2 SUN OS system patch level for non-integrated components

Network Element	OS Level
VitalQIP Enterprise	Solaris 10 Generic_127111-09
VitalQIP DNS	Solaris 10 Generic_127111-09
1310 OMC-P	Solaris 10 Generic_127111-09

Hardware requirements

Specific hardware requirements are addressed by the network element level release notes and documentation.

Compatibility restrictions

Backward compatibility is supported for the IMS solution software upgrade sequence from IMS 07.04.01 to IMS 07.05.01. See the *IMS Solution 07.04.00 Software Upgrade* document, 275-100-035R07.04.00, and specific NE documentation for more information. The specific upgrade path must be provided by each NE.

8 Installation and upgrade notes

Overview

Purpose

This chapter provides information on installation, upgrade procedures and security hardening.

Performing first-time installation

Contact your Alcatel-Lucent representative for first-time installation assistance.

Performing upgrades

The following solution-level document describes the recommended installation and upgrade sequence for the IMS network elements:

- *IMS Solution 07.04.00 Software Upgrade* 275-100-035R07.04.00

Upgrade paths

Upgrade to IMS 07.05.01 is supported from IMS 07.04.01. Network Elements may require multiple transitions to go from IMS 07.04.01 to IMS 07.05.01; refer to the specific NE documentation for further details.

Security hardening

IMS Release Network Element security hardening procedures and related information are on OLCS at: https://services.support.alcatel-lucent.com/services/.

Click on IMS Solutions, then click on the Security Hardening IMS Release and finally click on each NE for security hardening details.

A Release 07.05.01 Solution Documentation Impacts

Purpose

This appendix includes the Release 07.05.01-impacted sections of the *IMS Solution Technical Description* document, *IMS Solution Growth* document, *IMS Solution Interface Changes Specifications* document, *IMS Solution Ports and Protocols* document, and *IMS Solution System Parameters* document.

The following features impact the *Technical Description* document:

- 13987.30 – Presence Content XDMS (located on attached pages 3-27 – 3-31, 3-41 – 3-43, 3-108-109)
- 13987.31 – RCS 1.0 support by PS/XDMS 5.0 (located on attached pages 3-27 – 3-3, 3-41 – 3-431)
- 33333.235 – CPRS testing of VCC 8.0.2 with IMS 7.5
- 33333.243 – Test of NNI interface for XDMS 5.0 in IMS 8.2 (located on attached pages 3-29 – 3-31)
- 33333.255 – RCS 1.0 Testing of Tri-Op Functions (located on attached pages 3-108 – 3-109, 10-23 – 10-24)
- 33333.259 – AKA/Ipsec testing with 1440 USDS in IMS 7.5 (located on pages 6-8 – 6-11, 6-28 – 6-29)
- 33333.263 - CPRS testing of PS/XDMS 5.0 on HP platform in IMS 7.5/IMS 8.2 (located on pages 8-8 – 8-12, 8-18 – 8-23, 8-30 – 8-37)
- 33333.264 – E2E testing of 7510 in bearer path for Video Sessions in IMS 7.5 (located on pages 3-94 – 3-95, 3-108 – 3-109, 10-21 – 10-22)

The *Growth* document is impacted on the following pages:

- 4-4 – 4-7

The *Interface Changes Specifications* document is impacted on the following pages:

- 1-4 – 1-7

The *Ports and Protocols* document is impacted on the following pages:

- 1-1 -1-2, 2-1 – 2-2, 3-1, 4-1 – 4-2, 5-1 – 5-2

The *System Parameters* document is impacted on the following pages:

- 1-2, 2-2, 3-2, 4-2, 4-6

5410 PS

Purpose

This topic describes the 5410 Presence Server (PS).

Functions

The 5410 PS is a SIP application server in the IMS reference model.

The following services are provided by the 5410 PS:

- Presence services in accordance with the Open Mobile Alliance Presence Model
- Interoperability between servers and devices for managing user presence information
- Service enabler for other services which can retrieve presence information to enhance a service

The 5410 PS provides the following functions:

Functions	Description
PS	• Collects presence information from presentities and notifies watchers. • A presentity is a person, service, or device that publishes presence information to a presence server. • A watcher requests presence information from a presence server, it provides requested information to watcher • Allows the subscriber to publish a link to their status-icon in their presence information to support the dynamic avatar (icon) feature in Rich Communication Suite.
Resource List Server	Manages subscriptions to presence lists (resource-lists), which enables a watcher application to subscribe to the presence information of multiple presentities using a single subscription transaction.
Access control	Applies presence rules. Presence rules define access policies for subscriptions.
Presence Network Agent (PNA)	Collects presence information from network equipment.
Presence User Agent (PUA)	Collects presence information about presentity.

The 5410 PS provides the following services to support RCS 1.0:

- Store and notify presence information of all contacts in the contact list
- Store and Notify status-icon link to support dynamic avatar (icon)
- Store and notify the person elements in the presence document

- Store and notify the permanent presence state
- Handle anonymous authorization rule

Supported hardware platforms

The 5410 PS runs on the 5400 Advanced Telecommunications Computing Architecture (ATCA) platform and HP DL380.

Supported interfaces

The 5410 PS supports the following interfaces:

Interface	between...	and...
ISC	S-CSCF	5410 PS
Ma	I-CSCF	5410 PS
Pen (SIP)	PNA	5410 PS
Peu (SIP)	PS	PUA
SNMP (fault management, performance management)	5410 PS	1300 XMC

Supported northbound systems

The 1300 XMC provides fault management and performance management functionality for the 5410 PS.

The 5410 PS is managed using a GUI. This interface is based on the 5400 IAS GUI. The 5410 PS provides an additional GUI, which is integrated in the 5400 IAS GUI.

Charging

The 5410 PS does not support charging.

Product documentation

For details on the product and a full list of Presence-related specifications, refer to *Alcatel-Lucent 5410 Presence Server Reference Guide,* 3BL 76751 0401 RKZZA.

5410 XDMS

Purpose

This topic describes the 5410 Extensible Markup Language (XML) Document Management Server (XDMS).

Functions

The 5410 XDMS is a SIP application server and also an XCAP server in the IMS reference model.

The 5410 XDMS provides the following functions.

- Functionality for contact lists.
- Users can create and maintain address lists that are accessible from any service and from any device. It provides interoperability between servers and devices for managing user information.
  The search function has the capability of searching for user profiles (in shared profile, XDMS) and searching for groups of users (in shared group, XDMS).
- Acts as a service enabler for other services which can retrieve presence information to enhance a service.
  Stores and handles access to presence authorization rules, contact lists, user profiles, and shared groups.
- Retrieves and stores the status-icon in the Presence content XDMS to support the dynamic avatar (icon) feature in Rich Communication Suite.
- The XDMS shared group manages new XML shared group document and associated extended group advertisements. The 5410 XDMS includes an Aggregation proxy to route XCAP requests to the proper XDMS servers.

The 5410 XDMS provides the following services to support RCS 1.0:

- Store and retrieve the status-icon in the Presence content XDMS to support the dynamic avatar (icon) feature.
- Retrieve the status-icon information from an XDMS located in another operator’s network. For this purpose, the 5410 XDMS includes Cross network proxy.
- Support telephone URI in international public telecommunication number format.
- Store the presence authorization rules.
- Maintain the rcs list that includes all the authorized contacts of the user.

Aggregation proxy

The Aggregation proxy is the only contact point for the XDM client to access XML documents stored in XDMS.

The Aggregation proxy performs the following functions:

- User authentication using the HTTP Digest authentication scheme
- External authentication mapping using the CustomPatchProxylet to retrieve the user identity from the header set
- Alias management
- Routing XCAP requests to the XDMS or to the Cross Network proxy
- OMA directory processing to build the final response to the XDM client
- XCAP-capabilities processing to build the final response to the XDM client
- Tracking XCAP requests using access logs
- Forwarding search requests and search responses between the client and the search function

Cross network proxy

The Cross network proxy acts as a single point to handle XCAP requests over trusted connections between two networks.

The Cross network proxy performs the following functions:

- Authorization of trusted network
- Routing individual outgoing XCAP requests to the Cross network proxy of the remote network
- Routing individual incoming XCAP responses to the Aggregation proxy
- Secured data transfer between two networks

Supported hardware platforms

The 5410 XDMS runs on the 5400 Advanced Telecommunications Computing Architecture (ATCA) IMS Application Server (AS) and HP DL380.

Supported interfaces

The 5410 XDMS supports the following interfaces:

Interface	between...	and...
ISC	S-CSCF	5410 XDMS
Ma interface	I-CSCF	5410 XDMS
SNMP (fault management, performance management)	5410 XDMS	1300 XMC
Ut (XCAP)	5410 XDMS	UE
XCAP	5410 XDMS	Acme Packet® Net-Net® Session Director

Interface	between...	and...
SIP	5410 XDMS	7510 MG

Supported northbound systems

The 1300 XMC provides fault management and performance management functionality for the 5410 XDMS.

The 5410 XDMS has a native web-based GUI that supports configuration management functionality.

Charging

The 5410 XDMS does not support charging.

Product documentation

For more information on the 5410 XDMS, refer to the *A5350 XDMS Reference Guide,* 3BL 77755 0400 RKZZA.

Rich Communication Suite

What is RCS?

Starting with IMS Release 7.1, the Alcatel-Lucent IMS architecture is compatible with Rich Communication Suite (RCS) 1.0.

RCS is an industry effort focused on the use of IMS for enabling mobile phones with rich communication.

Services

RCS phase 1.0 provides the following services:

- Enhanced Address Book: Presence information integrated into the phonebook interface.
- Presence information with dynamic avatar (icon) supported by Presence Content XDMS.
- Sharing of social presence information with a list of contacts agreed by the subscriber.
- Fetching capability of all contacts in the contact list.
- File transfer as in Open Mobile Alliance (OMA) Instant Messaging (IM) SIMPLE 1.0.
- Peer-to-peer chat service and Group chat:
  - Ad hoc group messaging session as in OMA IM SIP SIMPLE 1.0
- Content Sharing:
  - Video Share
  - Image Share
- Enhanced services:
  - Hyper Availability to express the desire of the subscriber to communicate with contacts in the contact list.
  - Permanent presence state
  - Presence authorization rules such as Anonymous authorization rule, Own authorization rule, Default presence authorization rule
  - Favourite link setting
  - Note with a maximum of 100 characters along with emoticons

Capabilities

RCS provides the following capabilities:

- Wide and large-scale IMS deployment
- Inter-operability between different terminal vendor RCS clients
- RCS service inter-working between operators

Supported access networks

RCS supports the following access networks:

- WCDMA
- EDGE

Supported application servers

The Alcatel-Lucent RCS is supported by the following application servers:

- 5410 PS
- 5410 XDMS
- 5430 MMIM

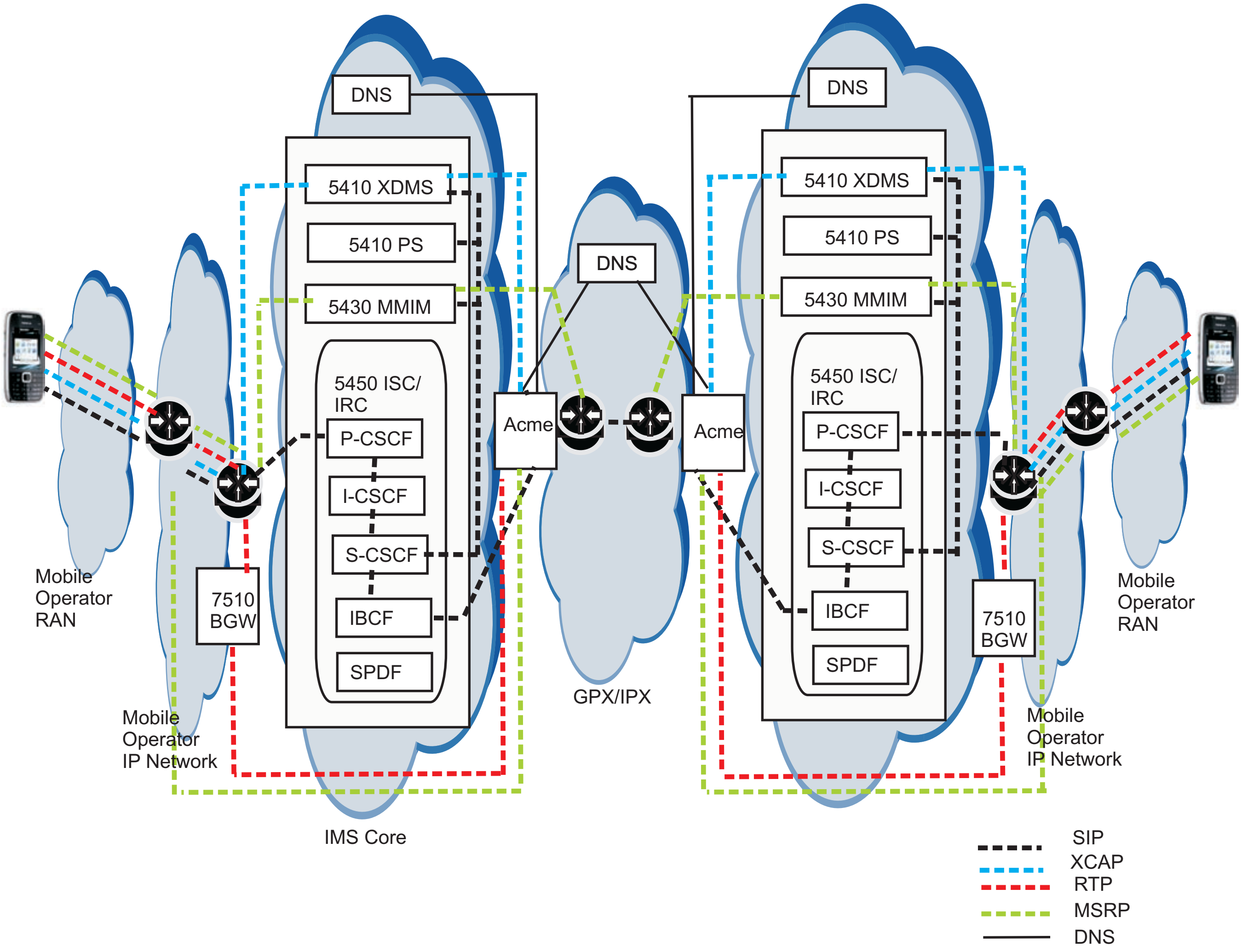
Standard compliance

The RCS supporting application servers 5410 PS, 5410 XDMS, and the 5440 PC Client are compliant with OMA release V1.1 and to the standards that are referenced by OMA release V1.1 for the Presence and XDMS services.

The 5410 XDMS and the 5440 PC Client are also compliant with OMA V2.0 limited to status-icon handling.

Supported architecture

The RCS supports the following architecture:



Supported clients and terminals

The Alcatel-Lucent RCS is supported by the 5440 PC Client.

The Alcatel-Lucent RCS solution is inter-operable with RCS phase 1.0 compliant terminals.

References

Refer to the 5410 PS, 5410 XDMS, 5430 MMIM, and 5440 PC Client product descriptions.

RCS services

Purpose

This topic provides general descriptions of the Rich Communication Suite services that are supported in IMS.

Supported services

The following services are supported in RCS 1.0:

- Address book
- File transfer
- Messaging services
- Content sharing services

Address book

The address book stores the details of all the contacts in the contact list along with dynamic presence information. The RCS supports the contacts with the international public telecommunication number format.

The RCS provides the following address book services:

- Enhanced address book
- Network address book

Enhanced address book

The enhanced address book stores the contact details and the presence information related to overriding willingness and hyper availability, status-icon, homepage, the note, and the emoticons. The enhanced address book also stores the supported services for the subscriber. The subscriber can make a call or start a chat session using the contact details in the enhanced address book.

Network address book

The network address book stores the published profile of all the subscribers in the network. The subscribers can retrieve a contact's published profile from the network address book, but cannot make any changes to the published profile on the network.

File transfer

The file transfer service helps the subscribers to send and receive files from the contacts in the contact list. The subscriber can send a file to multiple contacts. A dedicated SIP session and MSRP connection is established to transfer the file. The RCS supports the file transfer even when the sender or the receiver is involved in a chat session.

Messaging services

The messaging services allow the subscribers to send and receive instant messages, SMS, and MMS to the contacts stored in the address book.

Content sharing

The RCS supports the following sharing services:

- Video share
- Image share

Video share

The video share service helps the subscribers to establish a video share call and transfer the video. The shared video can either be a pre-stored video or live video. The video transfer is initiated either by the subscriber or by the called party.

Image share

The image share service helps the subscribers to establish an image share call transfer the image. The image share is initiated either by the subscriber or by the called party.

Products supporting RCS services

Service	Product
Address book service with presence information	5410 PS
File transfer	Supported by core IMS network
Messaging services	Supported by core IMS network

5440 PC Client

Purpose

This topic describes the 5440 PC Client.

Functions

The 5440 PC Client is a PC-based application that offers instant communication services such as voice and video telephony to end users (subscribers).

The 5440 PC Client provides the following services:

- Audio calls
- Video calls
- Video share with support for separate audio and video sessions
- Peer to peer file transfer
- Call log, call forwarding, call blocking
- Personal address book with presence information and dynamic avatar (icon)
- Personal profile
- Messaging including instant messaging, SMS, and MMS
- History of audio, video and messaging sessions
- MS outlook add-in to access 5440 PC Client from MS Outlook
- Anydial add-in to place calls to a valid phone number on a web page

The 5440 PC Client supports the following services in RCS 1.0:

- Sharing of social presence information with a list of contacts agreed by the subscriber.
- Presence information with dynamic avatar (icon) supported by Presence Content XDMS.
- Subscribers with telephone URI in international public telecommunication number format.
- Overriding willingness and hyper availability
- Favourite link (e.g. Homepage)
- Presence caching and persistence data
- Anonymous service retrieval

The 5440 PC Client has an integrated soft phone for voice and video calls. However, the client can be deployed without the integrated soft phone, in which case calls can be made using the associated phone.

The 5440 PC Client interacts with the 5430 MMIM server to provide messaging services.

Supported hardware platform

The 5440 PC Client is installed on the end user's PC operating on Microsoft Windows 2000, XP, or Vista.

Supported interfaces

The 5440 PC Client supports the following interfaces:

Interface	between...	and...
SIP	5440 PC Client	5410 PS
SIP , XCAP	5440 PC Client	5410 XDMS
HTTP, HTTPs	5440 PC Client	5420 PCM
SIP	5440 PC Client	5420 CTS
SIP, MSRP	5440 PC Client	5430 MMIM

Supported northbound systems

The northbound systems are not applicable for the 5440 PC Client.

Charging

The 5440 PC Client does not perform any charging function.

Product documentation

For more information on 5440 PC Client, refer to the *5440 PC Client User Guide,* 270-713-051.

7510 MGW

Purpose

This topic describes the 7510 Media Gateway (MGW).

Functions

The 7510 MGW provides the following functions:

- VoIP termination, providing access for SIP clients.
- VoIP trunking, providing IP-based connections for transit traffic.
- Centralized Access Gateway, providing PBX access to users in private TDM networks and PSTN.
- Internet offload, allowing traffic that is destined for the internet to be offloaded from the PSTN.
- TDM-to-TDM hairpinning, providing switching between local exchanges that are connected to the media gateway. Hairpinning ensures the IP network is not burdened with local calls.
- Supports audio and video sessions with multiple streams by providing a latching function for audio and video streams.

Supported hardware platforms

The 7510 MGW consists of modules in a chassis. The chassis are mounted in a standard telecommunication rack.

Supported interfaces

The 7510 MGW supports the following interfaces:

Interface	between...	and...
Mn (H.248)	7510 MGW	MGCF
Circuit interfaces, including: • STM-1/OC-3 • E1/T1 • PRI	7510 MGW	TDM based access nodes and users
SNMP (fault management)	7510 MGW	1300 XMC Northbound OSS
XML FTP (performance management)	7510 MGW	1300 XMC Northbound OSS

Supported northbound network elements

The 1300 XMC provides fault management, configuration management, and performance management functionality for the 7510 MGW.

The 7510 MGW local GUI provides configuration management functionality.

Charging

The 7510 MGW does not provide charging functionality.

Product documentation

For details on the 7510 MGW, refer to *Alcatel -Lucent 7510 Media Gateway Product Description,* 3FZ08014AAAPDEZZA .

Video services

Purpose

This topic provides general descriptions of video services that are supported in the IMS and provides short descriptions of the services themselves.

Peer-to-Peer Video Streaming

The Peer-to-Peer Video Streaming (PPVS) service allows a user to send video images to a contact. The PPVS service offers simplex (one way only) communication. A PPVS session does not allow the contact to send back video images. A video stream can be active in parallel with a voice call.

The PPVS service does not make use of any external application servers to provide services. The PPVS service is based on peer-to-peer simplex telephony (Voice over IP) using the IMS core network and complies with IETF SIP and 3GPP standards.

Video sessions with multiple streams are supported by 7510 MGW in the bearer path.

Starting with IMS 8.1, the IMS core can support video and audio streaming simultaneously.

Push-to-Show

The Push-to-Show (PtS) service allows users to stream video content in half duplex, near-real time. The Push to Show service is similar to Push-to-Talk, but uses video instead of voice.

Video conferencing

Video conferencing uses an external video conferencing application server to set up and manage video conferences.

Video telephony

Video telephony allows for video telephony over high rate packet data (HRPD).

Video mail

Video mail allows users to deposit and retrieve video messages. A caller with a video-enabled handset can leave a video mail message for another user that has video mail. The caller is presented with a video mail greeting and can then leave a video mail message.

Conferencing products and conferencing services

Service	Product
Peer-to-Peer Video Streaming	Supported by core IMS network
Push-to-Show	5430 Push-to-X
Video conferencing	Polycom video
Video telephony	5100 CMS Video Mail DOrA handset with a VT IMS client
Video mail	5100 CMS

UE registration message flow (using AKA)

Purpose

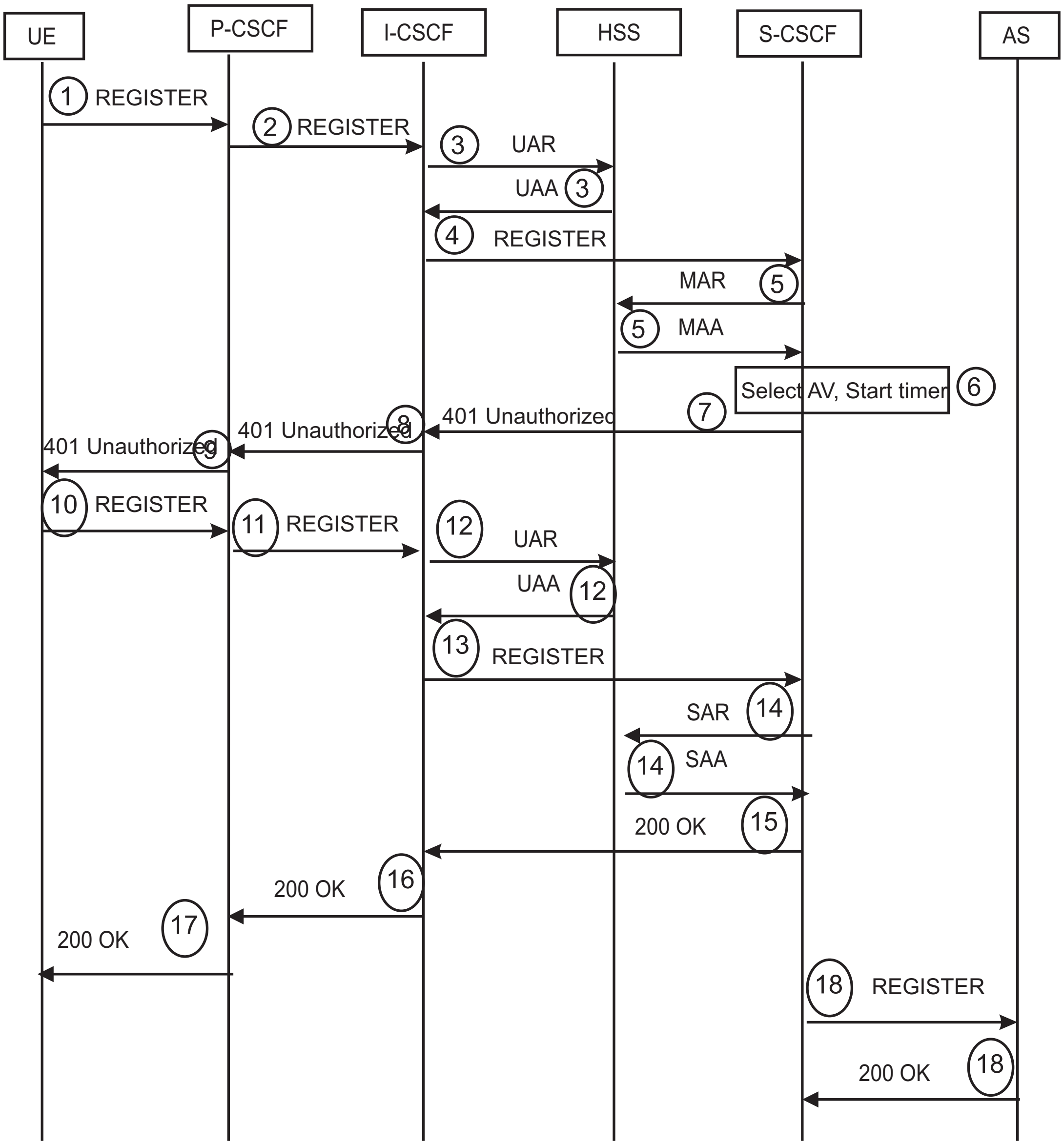
This topic describes how a SIP UE registers with the S-CSCF when the AKA authentication scheme is used.

Note: When the AKA authentication scheme is used, mutual authentication is performed for every unprotected REGISTER request. For protected REGISTER requests, the S-CSCF authenticates the UE depending on the operator's policy.

Reference: For more information on the AKA authentication scheme, refer to the IMS authentication schemes section in Chapter 7, Security.

UE registration message flow

The following message flow describes a SIP initial registration with an application server:



UE registration message flow description

The following description provides the stages of a SIP UE registration:

1 The UE, without an existing Security association (SA), sends an unprotected REGISTER message to the P-CSCF.

2 The P-CSCF in the visited network performs a DNS lookup to find the address of the I-CSCF in the home network. The P-CSCF forwards the REGISTER message to the I-CSCF.

3 The I-CSCF queries the HSS to get the status of the subscriber registration using a User authentication request (UAR) message. The HSS responds to the I-CSCF with User authentication answer (UAA).

4 Based on the information returned by the HSS, the I-CSCF selects an S-CSCF and forwards the REGISTER message to the selected S-CSCF.

5 The S-CSCF queries the HSS to authenticate the subscriber using a Message authentication request (MAR). The HSS responds to the I-CSCF with a Message authentication answer (MAA).

If...	Then...
The IMPI is registered	The S-CSCF downloads the authentication information form the HSS.
The PUID is not registered	The HSS sets the reg-flat attribute to **`init-reg-pending`**.

6 The S-CSCF selects an appropriate Authentication vector (AV). At this point, the S-CSCF starts the timer with the **`reg-await-auth`** attribute.

7 The S-CSCF sends a `401 unauthorized` message containing RAND, AUTN, IK, and CK attributes to the I-CSCF.

8 The I-CSCF forwards the `401 unauthorized` message to the P-CSCF.

9 The P-CSCF stores the IK and CK attributes mentioned in the `401 unauthorized` message and sets up a temporary SA with the SA lifetime equivalent to the reg-await-auth attribute.

The P-CSCF forwards the unprotected 401 unauthorized message to the UE.

10 The UE sets up a temporary SA and sends a protected REGISTER message containing the RES attribute and the temporary SA to the P-CSCF.

11 The P-CSCF validates the SA and its integrity. The P-CSCF also does a DNS query to find the address of the I-CSCF. The P-CSCF then forwards the REGISTER message to the I-CSCF.

12 The I-CSCF authenticates the UE by sending a UAR to the HSS. The HSS responds with a UAA.

13 The I-CSCF forwards the REGISTER message to the S-CSCF. At this point, the **`reg-await-auth timer`** stops.

14 The S-CSCF verifies the RES attribute in the REGISTER message and downloads the service profile from the HSS. The S-CSCF sends a SAR to the HSS and the HSS responds with a SAA. The HSS sets the Reg-flat attribute to registered.

Thus, the S-CSCF creates a binding with the UE and stores the service profile.

15 The S-CSCF sends a `200 OK` message to the I-CSCF.

16 The I-CSCF forwards the `200 OK` message to the P-CSCF.

17 The P-CSCF changes the temporary SA to an established SA and forwards the `protected 200 OK` message to the UE.

The UE changes the temporary SA to an established SA. Subsequent SIP messages will be protected with the established SA information.

18 The S-CSCF sends a third party REGISTER message to the AS and the AS responds with a `200 OK` message.

UE de-registration message flow (using AKA)

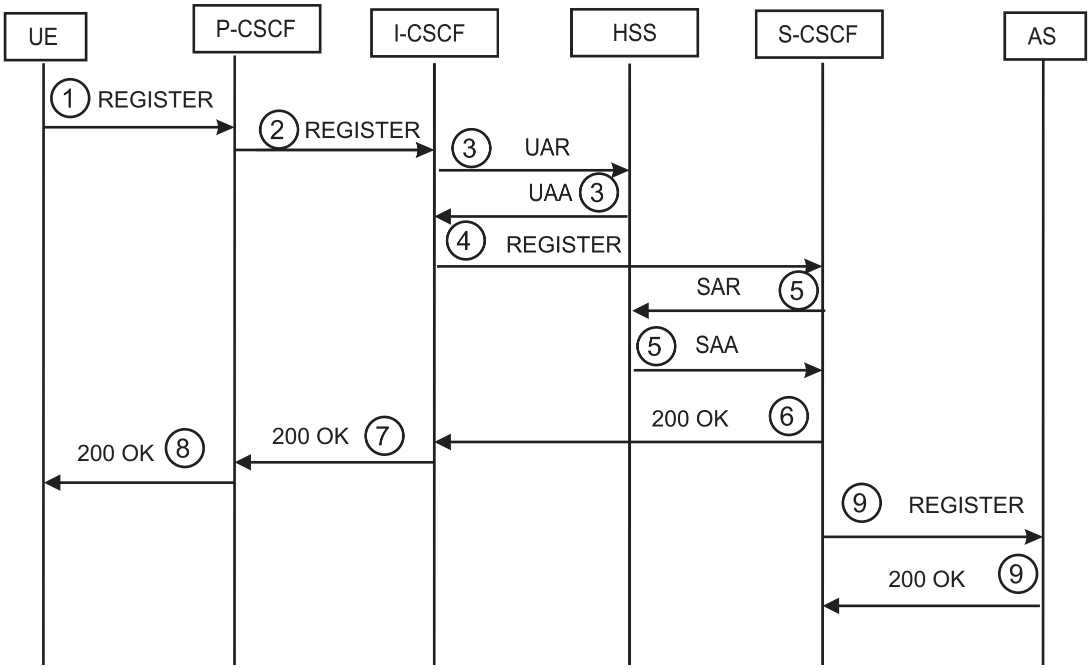
Purpose

This topic describes the message flow for a SIP UE de-registration process when the AKA authentication scheme is used.

Reference: For more information on the AKA authentication scheme, refer to the IMS authentication schemes section in Chapter 7, Security.

UE registration message flow

The following message flow describes a SIP UE de-registration with an application server:



UE registration message flow description

The following description provides the stages of a SIP UE de-registration:

1 The UE sends a REGISTER message with the existing SA information and the **`expire`** attribute set to zero to the P-CSCF.

2 The P-CSCF performs a DNS lookup to find the address of the I-CSCF. The P-CSCF validates the SA and its integrity. The P-CSCF then forwards the REGISTER message to the I-CSCF.

3 The I-CSCF queries the HSS to get the status of the subscriber registration using a User authentication request (UAR) message. The HSS responds to the I-CSCF with User authentication answer (UAA) which contains the address of the S-CSCF where the UE is registered.

4 The I-CSCF then forwards the REGISTER message to the S-CSCF.

5 The S-CSCF decides not to authenticate the UE. The S-CSCF queries the HSS to authenticate the services provisioned for the UE. The S-CSCF sends an SAR to the HSS and the HSS responds to the S-CSCF with an SAA. The S-CSCF then releases all the sessions for the UE and deletes the binding with the UE.

6 The S-CSCF sends a `200 OK` message with expires attribute set to zero to the I-CSCF.

7 The I-CSCF forwards the `200 OK` message to the P-CSCF.

8 The P-CSCF removes the binding with the UE and forwards the message to the UE. If all the IMPUs belonging to the UE are de-registered, the UE removes all the SA information.

9 The S-CSCF sends a REGISTER message with expires attribute set to zero to the AS and the AS responds with a `200 OK` message.

5420 VCC

Purpose

This topic describes the 5420 Voice Call Continuity (5420 VCC).

Functions

The 5420 VCC is an application server that provides Voice Call Continuity services. Voice Call Continuity allows a user to roam between an IMS (Wifi) network and a GSM network using a single handset. The handset is capable of connecting to both networks.

The 5420 VCC is available in small and medium configurations.

The 5420 VCC provides the following functions:

- Deliver calls depending on presence
  When the user has WiFi coverage, an incoming call is delivered to the IMS network.
- Handover calls between GSM network and WiFi network
  When the users moves from a GSM network into WiFi coverage, the call is handed over from GSM to IMS.

The 5420 VCC also supports the following functionality:

Call anchoring functionality

Regardless of the network that the user is connected to, the IMS controls the call. Control by IMS is provided by “anchoring”. Anchoring forces GSM originating and GSM terminating calls through the IMS.

In IMS 7.1, the anchoring decision also takes into account the emergency number and the call type. The 5420 VCC also offers the possibility of rerouting the call in case of non-availability of the IMS domain. As an option, location information can be provided to an AS in the operator network.

Fixed mobile convergence functionality

The 5420 VCC in IMS 7.1 provided capabilities supporting fixed mobile convergence. Users can roam freely between a broadband fixed network in an office or residence and a mobile network using one mobile phone number. A wireline phone (business desk phone in a centrex group or a home phone) or a PC on the broadband fixed network is treated as an extension of the mobile phone and is accessed through extension dialing.

This is an important added value that allows service providers to compete aggressively against free internet calling services which requires a second number to be assigned to the PC. The fixed mobile convergence capabilities of the 5420 VCC enable users to make and receive calls on their mobile phone or PC using the same phone number.

Supported hardware platforms

The 5420 VCC runs on an ATCA-based platform, the 5400 IAS.

Supported interfaces

The 5420 VCC supports the following interfaces:

Interface	between...	and...
FTP (performance management)	5400 IAS/5420 VCC	northbound systems
ISC	5420 VCC	S-CSCF
Ma	5420 VCC	I-CSCF
Rf	5400 IAS/5420 VCC	8615 IeCCF
Rp	5420 VCC	1440 USDS
Sh	5420 VCC	8650 SDM
SNMP (fault management)	5400 IAS/5420 VCC	northbound systems

Supported northbound network elements

An SNMP northbound interface is provided by the 5400 IAS platform. The 5400 IAS also stores measurements for the 5420 VCC application.

The 5400 IAS stores records that are retrieved using FTP or transferred using the Rf interface.

In IMS 7.x and 6.x, the user profile data for 5420 VCC was stored in the 1440 USDS and therefore the 5420 VCC was not provisioned with per subscriber data. The per subscriber data needed by the 5420 VCC was provisioned on the 1440 USDS. The eSM supported 5420 VCC (via the 1440 USDS) in IMS release 6.x. For IMS 7.0, the 8690 GUP had an Rp interface to 1440 USDS for subscriber provisioning. For IMS 7.1, the eSM supports 5420 VCC via the 1440 USDS.

Charging

Records are stored on the 5400 IAS and can be retrieved by an external system using FTP.

The 5420 VCC has an Rf interface to 8615 IeCCF for offline charging.

Product documentation

For details on the 5420 VCC, refer to *Alcatel-Lucent 5420 Voice Call Continuity Reference Guide,* 270-705-002.

Overload control

Overview

Overload occurs when a network element that is responsible for a functionality, experiences higher demand for that functionality than what is expected or engineered for that network element.

Overload control monitors Network Element (NE) functionality, detects when the system is becoming overloaded, and sets into place actions to address the overload. This section provides information about overload control in various NEs.

Overload control main areas

Overload control comprises the following areas:

- Detection, which includes monitoring the system for utilization of resources such as CPU, memory, or messages
- Isolation, which determines the root cause for the problem
- Correction, which takes corrective actions to limit the overload

Most network elements follow this approach. The implementation of the areas differs between network elements.

Operations and Maintenance Center – HLR and HSS (1440 OMC-H)

The SS7 network is the interface between the S-DHLR network element and the wireless operators' networks. The SS7 network interacts with the HLR control function (HCF) network elements. The 1440 USDS interacts with SS7 when sending and receiving messages to and from other elements within the network. The message types could consist of mobile equipment locations, updates, and requests for authentication verification.

The Overload is a container object and a child of the SS7. The Overload object allows finer control of the overload thresholds for all SS7 messages than that provided by the system defaults. The Overload Control is a managed object and a child of the Overload object, and defines the Transaction Capabilities Application Part (TCAP) automatic call gapping parameters for the HCF Cluster.

References

Refer to the following topics in the chapter, *Provision the SS7 network,* of the *1440 Operations and Maintenance Center–HLR and HSS (1440 OMC-H) Configuration Manager,* 401-380-078:

- Overload object description
- Overload Control object description
- SSN Overload Control object description

1310 OMC-P

The 1310 OMC-P does not provide overload control.

eSM

In the Enhanced Services Manager (eSM), overload means that too many provisioning requests are coming in. Work orders that flow in at a rate greater than the purchased eSM transactions per hour (TPH) are "queued" by the Work Order Manager process. The overload control mechanism temporarily suspends the in-take of work orders by the Work Order Manager from the validation queue until the overload condition is resolved. The Work Order Validation queue continues to accept incoming work orders from the eSM GUI users and upstream systems as long as room remains in the queue. When the maximum number of allowed users is reached, the eSM does not allow any more users to log into the eSM and the user receives an appropriate warning message.

References

Refer to the chapter, *Work Load Queues,* of the *Intelligent Network (IN) Enhanced Services Manager (eSM) Monitoring the System,* 270-720-334.

IN RC/V

Recent Change and Verify (RC/V) is used to modify the databases on the MiLife Application Server (MAS), Enhanced Control Server (eCS) and the Enhanced Control Server LE (eCS LE). There are forms and procedures for setting performance thresholds and priorities, optimizing timing, and configuring other parameters to optimize the capabilities of the eCS.

References

Refer to the chapter, *Configuring the SS7 platform,* of the *Intelligent Network (IN) Recent Change and Verify,* 270-780-422.

1440 USDS

As a distributed system, the 1440 Unified Subscriber Data Server needs an overall overload control strategy to remain stable and reliable. 1440 USDS overload control is divided into the following functions:

- HDF overload control - In HDF, the heartbeat thread monitors the HDF internal queue and the queue between HCF and HDF to determine current HDF overload level. The HDF node also has a self-protect mechanism. It tracks HDF internal queue overload status to decide whether or not to drop the massage by simply returning an error back to HCF node.
- HCF overload control – HCF has an Index Server and a Service Dispatcher to control overload.

References

Refer to the chapter, *Provision protocol independent features,* in the *1440 Unified Subscriber Data Server (USDS) Data and Provisioning Guide,* 270-710-920.

Alcatel-Lucent Control Platform

The Alcatel-Lucent Control Platform-based products include 5450 ISC , Service Broker, and 5420 CTS.

P-CSCF (A-LCP) provides interface functionality to UEs and could experience overload because too many UEs are requesting service, or too many UEs are using high message volume applications.

The ACC Remote Overload Control screen is used to configure Automatic Congestion Control (ACC) Remote Overload Control (ROC) parameters per stack/DPC.

References

Refer to the Part *System View*, *SS7 Device server*, *ACC Remote Overload Control Attributes* in *Alcatel-Lucent Control Platform - Object Descriptions,* 275-900-390.

Alcatel-Lucent Gateway Platform

The Alcatel-Lucent Gateway Platform-based products monitor resources, interfaces, and applications. When overload thresholds are crossed, alarms and SNMP messages are send to the 1310 OMC-P.

In 5400 Application Platform

Overload control is handled in the front end of the load balancing chain. A 503 Service Unavailable error in the HTTP and SIP protocols is returned when overload is detected. Overload detection is performed on the front end by the I/O Handler (load balancing) based on data returned by the Agents (application processes) on the CPU and Memory usage. In addition the I/O handler keeps tracks of the number of messages sent to an agent without acknowledgement. If it passes a certain tolerance rate that Agent is considered in overload and not included in the pool anymore for the new protocol sessions until it is no longer in overload.

5410 PS and 5410 XDMS

5410 PS and 5410 XDMS overload control relies completely on 5400 platform overload strategy. Overload control is handled in the front end of the load balancing chain. Overload detection is performed by the I/O handler or load balancer depending on the data returned by the call out agents on the CPU, Memory usage, and number of messages sent without acknowledgement.

For large configurations on 5400 ATCA platform, 5410 PS and 5410 XDMS applications run on separate callout agent blade and for small configurations both the applications run on a single callout agent blade. System capacity is grown by adding more callout agent blades into the load-shared pool.

5400 ISG

Overload in the 5400 Intelligent Services Gateway (ISG) is handled by the Framework Service Capability Server (SCS). The Service manager for each SCS is configured with load level thresholds. When the load that is handled by the service manager crosses a threshold, the service manager sends out a report to the Framework. When an SCS goes to severe overload, the Framework rejects new requests until the overload level drops.

For each SCS, you can define the load level thresholds and watermarks. Changes in SCS overload are reported as alarms.

References

Refer to the *MiLife Intelligent Services Gateway (ISG) User Status SCS User's Guide, ,* 270-300-080.

Alcatel-Lucent CM

The Alcatel-Lucent Communication Manager (Alcatel-Lucent CM) monitors resources to detect overloads. When the Alcatel-Lucent CM system detects an overload situation, the system goes into an overload protection status. In an overload protection status, the Alcatel-Lucent CM system rejects incoming requests from client application programming interfaces (APIs). Rejecting requests reduces the load on the system and allows the system to handle existing requests properly. The Alcatel-Lucent CM does not reject administration client API requests.

The Alcatel-Lucent CM reports overload conditions through SNMP traps. Thresholds can be configured for the SNMP traps.

The Alcatel-Lucent CM only rejects the following API requests:

- End-user client API requests
- Enterprise Administrator API requests

Administration client API requests are not rejected.

References

For more information, refer to related customer documentation.

5100 CMS

The Converged Messaging System (CMS) monitors CPU and disk usage, along with the incoming call rate per second, to determine if an overload state exists.

CMS overload or overflow conditions also occur when it cannot establish connections because no licenses or sessions are available.

When overload thresholds are reached or exceeded, overload alarms or overload events are generated. Depending on the overload condition and the priority of request, CMS rejects traffic.

You cannot configure overload thresholds.

References

For more information, refer to related customer documentation..

Local redundancy

Purpose

This topic provides an overview of the local redundancy schemes that are used in the network elements. The schemes that are used by the network elements provide a highly reliable IMS network.

Component level redundancy

The IMS network elements provide local or component level redundancy. Local or component level redundancy ensures that services are not lost when a hardware or software component of the network element fails.

The following are examples of component level redundancy:

- Dual power supply
- Card or module redundancy

Network element redundancy

The IMS network elements offer redundancy in case of failure of a complete server, chassis, or system.

The following are examples of network element redundancy:

- Servers in clusters
- Primary - alternate schemes, such as,
  - Active - Active
  - Active - Hot standby
  - Active - Warm standby
  - Active - Cold standby
  - Load-sharing (N+K)

The network element redundancy is also known as high availability (HA).

Servers in clusters

A server cluster consists of two or more independent servers. The servers work together as a single system providing a high level of availability, reliability and scalability. The workload is redistributed and resources are redirected when a server fails in the cluster.

Primary - Alternate schemes

In a primary and alternate site configuration, there is an element on location that handles live traffic. A standby or backup element in the same location is available to take over in case of a failure.

Data from the primary element is replicated on the backup element, either manually or automatically.

The different primary-alternate schemes for local redundancy are:

- **Active-Active:**
  An active component provides services, and constantly updates the other active component. The other active component takes over in case of a failure.
  Typically active-active scheme causes no loss of service. Active-active scheme is also known as 1:1.
- **Active-Standby:**
  An active component provides services the standby component takes over in case of failure. Typically active-standby scheme causes a short loss of service.
  - **Active-Hot standby:**
    The hot standby element is kept up-to-date with the active element in real time.
  - **Active-Warm standby:**
    The warm standby element is kept up-to-date with the active element in near real time.
  - **Active-Cold standby:**
    The cold standby element is kept up-to-date by periodically installing backups. Typically active-cold standby scheme requires manual procedures to install and configure the standby element
- **Load-sharing**
  N+K:
  Processing or traffic is distributed over multiple servers or hardware components. In case of failure, other components must provide sufficient resources to handle the increased load. K spare components are available to take over from failure of any of the N components
  Note: 1:N is a scenario where one spare component is available for N number of components. The spare component takes over from failure of any of the N components.

Within a network element, multiple local redundancy schemes can be used for different components.

For example: Active - Active scheme for some components and N+K scheme for other components.

Network elements redundancy schemes

The IMS network elements and their local redundancy schemes are listed in the following table

Network element	Used reliability schemes
Alcatel-Lucent Control Platform based products: • 5420 CTS • 5450 IRC • 5450 ISC	The Alcatel-Lucent control platform based products support the following scheme: • Active - Standby scheme for all components – Deployed on two fully redundant shelves
Alcatel-Lucent Gateway Platform based products: • 5020 MGC- 8 • 5025 VSG • 7520 MGW	The Alcatel-Lucent Gateway Platform based products supports the following scheme: • Active-Standby scheme: – 1:1 for essential components – N:1 for other components
1300 CMC	The 1300 CMC supports the following scheme: • N+1 mode here, N number of 5020 MGC-12 nodes are managed by one 1300 CMC server.
1300 XMC	The 1300 XMC supports the following scheme: • Active-Standby
1357 ULIS	The 1357 ULIS support the following schemes: • Active-Standby • The 1357 ULIS function (Interception management Center (IMC) and the Lawful Interception Gateway (LIG)) run on a two server cluster in Active - Standby mode
1440 OMC-H	The 1440 OMC-H support the following schemes: • No server redundancy • Redundancy for essential components on the server's hardware • Active-Cold standby
1440 USDS	The 1440 USDS support the following schemes: • N+K load sharing • 1:1 redundancy • Sparing

Network element	Used reliability schemes
5020 MGC – 12	The 5020 MGC-12 support the following schemes: • Active-Active • Active - Standby • Load-sharing
5060 MGC-10	The 5060 MGC-10 support the following schemes: • 1:1 Active-Hot standby • N+1 scheme with load sharing
5100 CMS	The 5100 CMS support the following schemes: • Active-Standby for all components • 1:1 load sharing
5400 IAS	The 5400 IAS support the following schemes: • N+1 redundancy with load balancing • Active-Standby mode
5400 ISG	The 5400 ISG supports the following scheme: • N+K load sharing
5420 PCM	The 5420 PCM support the following schemes: • 1+1 (active-standby) for some components • 1+1 (active-active) for some components • N+1 (active-active) for some components
5420 VCC	The 5420 VCC support the following schemes: • N+1 redundancy with load balancing is supported for some components • Active-Standby for some components • N+K redundancy scheme for some components
5450 AGCF	The 5450 AGCF supports the following scheme: • Active-Standby
5620 SAM	The 5620 SAM supports the following scheme: • Active-Standby
5900 MRF	The 5900 MRF support the following schemes: • Active-Standby scheme is used when MRFC and MRFP are located in the same server • Active-Standby scheme is used for standalone MRFC component • N+1 redundancy with load sharing is used for standalone MRFP component

Network element	Used reliability schemes
7510 MGW	The 7510 MGW supports the following scheme: • Active-Hot standby with load sharing – N+1 redundancy for some components – 1+1 redundancy for some components
7515 MGW	The 7515 MGW supports the following scheme: • Active-Standby
7302 ISAM-V	The 7302 ISAM-V supports the following scheme: • Active- Hot standby scheme is supported only for H248
8615 IeCCF	The 8615 IeCCF support the following schemes: • Active-Active load sharing • N+K redundancy
8650 SDM	The 8650 SDM supports the following scheme: • N+1 load sharing for some components • Active-Active load sharing for some components
8950 SAM	The 8950 SAM supports the following scheme: • Active-Standby
Alcatel-Lucent Communication Manager	The Alcatel-Lucent Communication Manager support the following schemes: • N+K load sharing • 1:1 (Active-Active)
eSM	The eSM support the following schemes: • Active--Standby server cluster • Redundancy for essential components on the server's hardware
1310 OMC-P	The 1310 OMC-P support the following schemes: • Active-Standby servers • Redundancy for essential components on the server's hardware
SMS	The SMS support the following schemes: • Redundant SMS servers in Active-Active scheme • Active-Active load sharing • Multi-SMS server cluster

Network element	Used reliability schemes
VitalQIP DNS	The VitalQIP DNS supports the following scheme: • Active-Hot standby
VPN Firewall Brick	The VPN Firewall Brick supports the following scheme: • Active-Standby Brick pairs
5400 Application Server Platform	The 5400 Application Server Platform supports the following schemes: • Pilot blades - active/standby • Application blades - N+K configuration • Database (MySQL) blades - active/standby
5410 PS and 5410 XDMS	5410 PS/XDMS support the following schemes: • The configuration on 5400 ATCA platform is supported on active call agents. • The configuration on HP platform, contains N+K load-shared active call agents and the redundancy is maintained between call agents for stable call retention.

References

Most network elements support multiple reliability schemes.

For details about the available reliability schemes and configurations, refer to the documentation set of the network element.

IMS network element redundancy schemes

Purpose

This topic describes the redundancy schemes that are available for the IMS network elements. A specific redundancy scheme is provisioned depending on the customer network and requirements.

Component level redundancy

Besides (geographic) redundancy for the network elements or systems, the network elements also provide local or component level redundancy.

When the tables list “No geographic redundancy”, the network element provides local redundancy.

Alcatel-Lucent CP-based network elements

The following redundancy schemes can be provisioned for the Alcatel-Lucent Control Platform-based network elements:

Network element	Redundancy scheme
5420 CTS	• No geographic redundancy • Primary - alternate scheme • Geographic redundancy N+K
5450 IRC	• Supports geographic redundancy • Primary - alternate scheme • Geographic redundancy N+K
5450 ISC	• Supports geographic redundancy • Primary - alternate scheme • Load-sharing scheme

References

For more information, refer to the section, *Geographical redundancy* in *Alcatel-Lucent Control Platform - Technical Description,* 275-900-320.

Alcatel-Lucent GP-based network elements

The following redundancy schemes can be provisioned for the Alcatel-Lucent Gateway Platform-based network elements:

Network element	Redundancy scheme
5020 MGC-8	• No geographic redundancy • Primary-alternate scheme For static data, 1310 OMC-P replicates the data on the standby 5020 MGC-8. For dynamic data, these is no replication of data between active and standby 5020 MGC-8. When standby 5020 MGC-8 takes over, it creates call state data based on the information received from 7520 MGW and 7510 MGW.
5025 VSG	• No geographic redundancy • Hybrid For static data, 1310 OMC-P replicates data on the standby 5025 VSG. For dynamic data, these is no replication of data between active and standby 5025 VSG. When standby 5025 VSG takes over, it initially assumes the state of SS7 network and retrieves the dynamic states from SS7 network. MTP L3 and above layer works in primary-alternate mode. MTP2 works in active-active mode.
7520 MGW	• No geographic redundancy. 7520 MGW does not provide geographic redundancy, but 5020 MGC-8 is provisioned with alternate routes and the trunk group is spanned across multiple media gateways. In case of media gateway failure, 5020 MGC-8 routes the call to another trunk within the trunk group to another 7520 MGW/7510 MGW or to an alternate route.

1357 ULIS

The 1357 ULIS does not support geographic redundancy.

1440 USDS

The following redundancy schemes can be provisioned for the 1440 USDS:

- No geographic redundancy
- Geographic redundancy with load sharing

The Hybrid Coordination Function (HCF) is implemented on the MiLife Application Server (MAS). The Application Server (AS) is deployed in an N+K configuration across locations. All servers handle traffic. If one or more servers (up to K) fail, the remaining servers can still handle the required traffic load.

The HLR Data Function (HDF) is implemented on a MAS that is deployed as a Data Server (DS). The Data Servers can be deployed in a mated pair or in stand-alone configuration. When the DSs are deployed in mated pairs, replication is supported using the TimesTen replication capability. This means that a hot standby is always available if one of the HDF nodes goes down.

References

For more information, refer to *Architecture overview,* in the *Product Overview,* 270-710-917.

5020 MGC – 12

The following redundancy schemes can be provisioned for the 5020 MGC-12:

- No geographic redundancy
- Active-active scheme
- Primary alternate scheme with active-warm standby. The managed elements can be located in the same site or geographically separated.

The 1300 CMC distributes the management data for FCAPS into the managed elements. The FCAPS data is individually considered for each interconnection point, which are the active network elements. The 1300 CMC replicates and synchronizes the databases and reports automatic switchover in case of failure.

References

Contact your Alcatel-Lucent customer team to obtain the documentation.

5060 MGC-10

The following redundancy schemes can be provisioned for the 5060 MGC-10:

- No geographic redundancy
- N+1 active-cold standby scheme
- Active-active scheme with load-sharing

References

Contact your Alcatel-Lucent customer team to obtain the documentation.

5100 CMS

The 5100 CMS does not currently support geographic redundancy.

5400 Application Server Platform

An individual application blade can participate in any of the following clusters:

- Application Server Runtime (ASR) I/O Handler Cluster - Not geographically distributable. These stateless blades can be configured locally in N+K configuration.
- SS7 I/O Handler Cluster - The SS7 cluster is a geographically distributable N+K cluster of blades that can use single point code access to the SS7 network.
- Agent Cluster - An agent cluster is a geographically distributable network of blades.
- Front End MySQL Database Cluster - The blades are stateless and can be geographically distributed in N+K form.
- Back End MySQL Database Cluster - By default, the 5400 platform uses this cluster with both local and geographically remote data distribution.
- ASR Control Blades Cluster - This is a pair of blades local to one site that control Agent installation, configuration and distribution for all of the agents across the network.

5410 PS and 5410 XDMS

5410 PS and 5410 XDMS currently do not support geographic redundancy.

5400 IAS

The 5400 IAS supports geographic redundancy.

References

Contact your Alcatel-Lucent customer team to obtain the documentation.

5400 ISG

The following redundancy schemes can be provisioned for the 5400 ISG:

- No geographic redundancy
- Geographic redundancy with load sharing

All Service Capability Servers (SCS)s can be deployed in a cluster with multiple instances of an SCS type (called clone).

The SCSs are simultaneously active and concurrently process transactions. All clones operate as independent autonomous entities. Each node can host at most one SCS of a given type.

The 5400 ISG cluster is deployed with an N+K architecture. The N MASs are deployed to provide the desired capacity and the K MASs to provide the required availability.

Some SCSs require data to be replicated across the MASs in the 5400 ISG configuration. Replication ensures that in case of a failure, the remaining clone of the SCS has the necessary data to continue processing client transactions. Since replication is required, TimesTen is used as the database.

References

For more information, refer to the *MiLife Intelligent Services Gateway (ISG) User Status SCS User's Guide,* 270-300-080.

5420 VCC

5420 VCC does not support geographic redundancy.

5450 AGCF

The following redundancy schemes can be provisioned for the 5400 ISG:

- No geographic redundancy
- Primary-alternate scheme with active-warm standby

References

For more information, refer to *Geographical redundancy* in the *Alcatel-Lucent AGCF Access Gateway Control Function System description,* 3EC 13643 BCAA TQZZA.

5620 SAM

The following redundancy schemes can be provisioned for the 7510 MGW:

- No geographic redundancy
- The 5620 SAM supports active-standby geographic redundancy.

The 5620 SAM redundancy is designed to remove single point failures in the server infrastructure, software and connectivity among servers. Additional external infrastructure is not required.

The 5620 SAM provides full status information to the operator regarding redundancy through its GUI interface and allows ‘controlled redundancy testing’ to ensure the integrity of the coverage.

References

For more information, refer to *Installation for 5620 SAM applications* in the *Alcatel 5620 Service Aware Manager Installation and Upgrade Guide,* 95-5813-01-00.

5900 MRF

5900 MRF does not support geographic redundancy.

7510 MGW

The following redundancy schemes can be provisioned for the 7510 MGW:

- No geographic redundancy
- The Alcatel-Lucent 7510 MGW can be partitioned into multiple Virtual Media Gateways (VMGs) allowing multiple controllers to interact simultaneously with disjoint sets of contexts/terminations within the same MGW. This MGC-12 multi-homing capability provides functionality for geographical redundancy in case of catastrophic outages at the call control layer (1 Media Gateway is controlled by 2 MGC-12 servers at different locations) as well as for efficiency (multiple MGC-12-entities can share resources of an Alcatel-Lucent 7510 MGW).
- The Alcatel-Lucent 7510 MGW supports geographic redundancy in a network. To enable a call server (MGCF, IBCF or SPDF) to synchronize the call-context related information via the 7510 MGW, the H.248.gri package is supported. Therefore the call server establishing new call contexts provides the 7510 MGW, call-context records per context. At failover, the redundant call server obtains these records from MGW, required for further call processing, while the bearer-path is kept up.

References

For more information, refer to *Alcatel-Lucent 7510 Media Gateway Product Description,* 3FZ 08014 AAAQ DEZZA.

7302 ISAM-V

7302 ISAM-V does not support geographic redundancy.

8615 IeCCF

The following redundancy schemes can be provisioned for the 8615 IeCCF:

- No geographic redundancy
- Load sharing

From an IMS network point of view, the IeCCFs are configured to share the load from network elements in the IMS network. The 5420 CTS and 5450 IP Session Control share IeCCF. From the 5420 CTS and 5450 IP Session Control perspective, the IeCCF systems act as primary-alternate systems. In case of failure of a IeCCF, an alternate IeCCF is used.

References

Contact your Alcatel-Lucent customer team to obtain the documentation.

8650 SDM

The following redundancy schemes can be provisioned for the 8650 SDM:

- No geographic redundancy
- Distributed configuration is always deployed as active-standby where the following are implemented:
  - N+K configuration (usually K=1) is supported for some components
  - Load shared redundancy is supported for some components
- Compact medium configuration is always deployed as mated pairs, this configuration supports active-standby redundancy
- Compact small configuration is always deployed as mated pairs, this configuration supports active-standby redundancy

The 8650 SDM supports active-standby geographic redundancy scheme.

References

Refer to *Overview of platform hardware* in the *Alcatel-Lucent 8650 Subscriber Data Manager SDM Maintenance,* 3BL 95528 BAAA PCZZA.

AcmePacket Net-Net® Session Director

The following redundancy schemes can be provisioned for the AcmePacket Net-Net® Session Director session border controller:

- No geographic redundancy
- Primary-alternate scheme

The Net-Net® SDs are deployed in pairs to provide High Availability (HA). The primary *Net-Net®* SD processes signaling and media traffic. The backup system is fully synchronized with the primary system. If the primary system detects service disruptions or degraded service levels, the primary system alerts the backup system to become active.

References

For more information, refer to *HA Nodes* in the Net-Net® *Session Director - Configuration Guide,* 400-0061-40A.

Alcatel-Lucent CM

The following redundancy schemes can be provisioned for the Alcatel-Lucent Communication Manager (Alcatel-Lucent CM):

- No geographic redundancy (simplex)
- Load sharing (high availability and geographical high availability)

References

For more information, refer to *Lucent CM system deployment* in the *Lucent Communication Manager Administration Guide,* 255-490-001.

BTS

The following redundancy schemes can be provisioned for the Billing and Traffic Server (BTS):

- No geographic redundancy
- Primary-alternate scheme

The Alcatel-Lucent Gateway Platform-based network elements are provisioned with a primary and an alternate BTS. If the network elements cannot transmit files to the primary BTS, the network elements use the alternate BTS.

References

Contact your Alcatel-Lucent customer team to obtain the documentation.

VitalQIP DNS

The following redundancy schemes can be provisioned for the VitalQIP Domain Name System (DNS):

- No geographic redundancy
- Primary-alternate scheme

VitalQIP offers a wide range of redundancy schemes, including single server or in multi-server environments.

References

For more information, refer to *Plan and configure your network* in the *VitalQIP Administrator Reference Manual,* 190-409-042.

VitalQIP ENUM

VitalQIP ENUM does not support geographic redundancy.

VPN Firewall Brick

Firewalls are always deployed on a specific location to protect that location. Firewalls do need a geographical redundancy scheme.

The following redundancy schemes can be provisioned for the VPN Firewall Brick:

- Primary-alternate scheme (with active-standby VPN Firewall Brick)

Two VPN Firewall Bricks can be deployed as a failover pair. The Bricks are identically configured, and share a single IP address. The standby Brick takes over when the active Brick fails.

References

For more information, refer to *Brick Failover* in the *Security Management Server SMS and Brick Redundancy Guide,* 260-100-007.

5420 CTS

Growth guidelines

In IMS, the 5420 Converged Telephony Server (CTS) is a Session Initiation Protocol (SIP) telephony application server.

Growing the 5420 CTS

While growing the 5420 CTS, the following considerations must be kept in mind:

- The 5420 CTS servers are addressed using a Fully Qualified Domain Name (FQDN), where the FQDN is defined as a domain name system record. The domain name system does not need to be updated with the Internet Protocol (IP) address(es) of the newly-grown hardware.
- The 5420 CTS servers must be defined in the Home Subscriber Server (HSS), created in initial Filter Criteria tables, and then subscribers must be assigned to the associated initial Filter Criteria.
- Update the Charging Collection Function (CCF) that allows the newly-added 5420 CTS to generate Accounting Request (ACR).

Updating the 5420 PCM

The 5420 PCM is an optional function of the 5420 CTS. The 5420 PCM can be used to activate and deactivate many 5420 CTS-based features and administer their associated data.

If the 5420 PCM supports 5420 CTS features, then the 5420 PCM must also be updated.

> **Note:** The 5420 PCM was moved out from 5420 CTS R6.2. The 5420 LCM is supported in 5420 CTS 6.2.1 but not in 5420 CTS 6.2. From 5420 CTS 7.0, the name is changed to 5420 PCM.

Updating the 1310 OMC-P to support new hardware

The 1310 OMC-P must be re-synchronized if a blade is added or a new CTS is grown or added to support the newly-grown hardware. A new blade or CTS data is populated via either *base_cfg.ksh* or via FSGUI. A configuration synchronization is needed so that the 1310 OMC-P is aware about the blade.

Provisioning via the 1310 OMC-P

The 8950 SAM provisions the 5420 CTS via the OMC-P. The 8950 SAM does not communicate with the 5420 CTS network elements directly and uses the OMC-P to provision the CTS.

The 8950 SAM must be connected to each of the 1310 OMC-P instances.

New Ethernet inter-connections

No new Ethernet inter-connections are required if you are growing a blade on an existing CP1800. New Ethernet inter-connections are required for new CP1800 instances.

Geographical-redundancy considerations

The 5420 CTS supports geographical-redundancy. If a CTS fails, it is isolated and will no longer be called by the 5450 ISC. The 5450 ISC calls an alternate CTS by the initial filter criteria. An interface between the primary and alternate CTSs keeps the subscriber data in sync. The growth is needed on both primary and protection sides.

Reference

For CP 1000 configurations, refer to *Part V, Configuration Management, Manage system configuration - hardware growth chapter* in *Alcatel-Lucent Control Platform 1000 Operations, Administration, Maintenance and Provisioning,* 275-900-882.

For CP 1800 configurations, refer to *Part V, Configuration Management, Manage system configuration - hardware growth chapter* in *Alcatel-Lucent Control Platform 1000/1800 Operations, Administration, Maintenance and Provisioning,* 275-900-872.

5410 PS

Growth guidelines

In IMS, the 5410 Presence Server (PS) is a SIP application server supporting presence services.

Note: Alcatel-Lucent Services performs hardware growth for the 5410 PS.

Growing the PS

The 5410 PS can be grown by the 5400 Advanced Telecommunications Computing Architecture (ATCA) platform growth and the HP DL380 growth.

The 5410 PS is grown in ATCA by adding new shelves or cabinets. The 5410 PS is grown in the HP platform by adding nodes. As new servers are added, the fully qualified domain name (FQDN) associated with these servers must be updated in the domain name system to allow the newly-grown server(s) to be accessed by other IMS elements. If existing FQDNs are used, no updates are required to the IMS elements. Once a new FQDN is introduced, IMS elements need to be updated to use the newly-created FQDN.

While growing the PS, add the IP at the FQDN for the OAM plane, so that it can communicate with the hosts individually. There is no impact on the signaling plane - all these new resources are sharing the same set of I/O handlers and the same FQDN. The DNS does not need to be updated as this is hidden to other nodes.

Updating the 1300 XMC

The 1300 XMC provides fault management and performance management functionality for the 5410 PS, so updates are required on the 1300 XMC.

New Ethernet connections

The 5410 PS connects to the core network via IP connections, so new Ethernet inter-connections are required.

Reference

Refer to the *Alcatel-Lucent 5410 Presence Server Reference Guide,* 3BL 76751 0401 RKZZA.

5410 XDMS

Growth guidelines

In IMS, the 5410 Extensible Markup Language (XML) Document Management Server (XDMS) is a SIP application server and an XML Configuration Access Protocol (XCAP) application server.

Note: Alcatel-Lucent Services performs hardware growth for the 5410 XDMS.

Growing the XDMS

The 5410 XDMS can be grown by the 5400 Advanced Telecommunications Computing Architecture (ATCA) platform growth and the HP DL380 growth.

The 5410 XDMS is grown in ATCA by adding new shelves or cabinets. The 5410 XDMS is grown in the HP platform by adding nodes. As new servers are added, the fully qualified domain name (FQDN) associated with these servers must be updated in the domain name system to allow the newly-grown server(s) to be accessed by other IMS elements. If existing FQDNs are used, no updates are required to the IMS elements. Once a new FQDN is introduced, IMS elements need to be updated to use the newly-created FQDN.

While growing the XDMS, add the IP at the FQDN for the OAM plane, so that it can communicate with the hosts individually. There is no impact on the signaling plane - all these new resources are sharing the same set of I/O handlers and the same FQDN. The DNS does not need to be updated as this is hidden to other nodes.

Updating the 1300 XMC

The 1300 XMC provides fault management and performance management functionality for the 5410 XDMS, so updates are required on the 1300 XMC.

New Ethernet connections

The 5410 XDMS connects to the core network via IP connections, so new Ethernet inter-connections are required.

Reference

Refer to the *Alcatel-Lucent 5410 XDMS Reference Guide,* 3BL 77755 0401 RKZZA.

5420 VCC

Growth guidelines

In IMS, the 5420 Voice Call Continuity (VCC) is an application server that provides Voice Call Continuity services.

Note: Alcatel-Lucent Services performs hardware growth for the 5420 VCC.

Growing the VCC

The 5420 VCC runs on the 5400 Advanced Telecommunications Computing Architecture (ATCA) platform.

The 5420 VCC is available in small and medium configurations. A small configuration can be grown to a medium configuration through the addition of ATCA cards. Additional growth requires additional systems such as another chassis and cabinet. Adding capacity can typically be done without impacting another network element.

The 5420 VCC FQDN is assigned by the network administrator. The iFC for a 5420 VCC subscriber and the DNS include the 5420 VCC FQDN.

OAM via the 5400 IAS

The 5400 ATCA IMS Integrated Application Server (IAS) that runs 5420 VCC provides an SNMP interface for fault management.

The 5400 ATCA IMS IAS stores 5420 VCC measurements.

Provisioning the 1440 USDS

The user profile data for 5420 VCC is stored in the 1440 USDS and therefore the 5420 VCC is not provisioned with per subscriber data. The per subscriber data needed by the 5420 VCC is provisioned on the 1440 USDS.

In IMS release 7.0, the 8690 GUP has an Rp interface to 1440 USDS for subscriber provisioning.

New Ethernet connections

The 5420 VCC connects to the core network via IP connections, so new Ethernet inter-connections are required.

Reference

Refer to *Chapter 5 5420 VCC Service Initiation* in the *Alcatel-Lucent 5420 Voice Call Continuity (VCC) Provisioning Guide,* 270-705-003.

Refer to *Chapter 5 Configuration Management* in the *Alcatel-Lucent 5420 Voice Call Continuity (VCC) Administration Guide,* 270-705-001.

Refer to *Appendix Installation Procedures* in the *Alcatel-Lucent 5400 ATCA Release 1.3x New Install Release Notes,* 270-700-229.

Summary of changed interfaces between release 07.04.00 and release 07.05.00

Purpose

This topic provides a summary of the changed interfaces between IMS release 07.04.00 and release 07.05.00.

Summary of interface changes

Important! A change in a network element software release does not automatically mean that the interfaces supported by the network element have changed.

The following table lists the network elements and indicates if their interfaces have changed between IMS release 07.04.00 and release 07.05.00:

Product	Product release for IMS 07.04.00	Product release for IMS 07.05.00	Supported interface(s)	Interface(s) changed • Y (yes) • N (no) • New (for new products in the IMS architecture)
1300 Convergent Network Management Center (CMC)	R2.1.7	R2.1.8	SNMP	N
			FTP	N
			SOAP XML	N
			HTTP/HTTPS	N
			MTOSI	N
			SFTP	Y
			LDAP	Y
			IPSEC	Y
1300 Cross Domain Management Center (XMC)	R6.2.2.5	R6.2.2.5	CORBA 3GPP	N
			HTTP/HTTPS	N
			SNMP	N
			SOAP/XML	N
			XML via FTP/Secure FTP	N

Product	Product release for IMS 07.04.00	Product release for IMS 07.05.00	Supported interface(s)	Interface(s) changed • Y (yes) • N (no) • New (for new products in the IMS architecture)
1310 Operations and Management Console - Provisioning (OMC-P)	13.0.1	13.2	SNMP	N
			XML	N
			FTP/Secure	N
			FTP	N
			FTP GET	N
			XML SOAP	N
1440 Operations and Maintenance Center - H (OMC-H)	R7.7	R7.7	ASCII	N
			SNMP	Y
			FTP/SFTP	N
			CORBA	N
			SSH	N
5020 Media Gateway Controller (MGC-12)	MGCSX30 NGVI SP2	MGCSX312 NGVI SP3	SNMP	N
			FTP/sFTP	N
5100 Converged Messaging System (CMS)	R10 SU3	R10 SU3	FTP	N
			SNMP	N
			HTTP/HTTP(s)	N
			LDAP	N
5400 IMS Application Server (IAS)	R1.3.3	R1.3.3	CORBA	N
			SOAP/XML	N
			FTP/SFTP	N
			SNMP	N
5400 Intelligent Services Gateway (ISG)	8.1	8.1	SNMP	N

Product	Product release for IMS 07.04.00	Product release for IMS 07.05.00	Supported interface(s)	Interface(s) changed • Y (yes) • N (no) • New (for new products in the IMS architecture)
7302/7330 Intelligent Services Access Manager - Voice (ISAM-V)	R3.7	R3.7	SNMP	N
8610 Instant Convergent Charging (ICC)	R4.6.2 Data MD02	R4.6.2 Data MD02	Ro (Diameter)	N
			SNMP	N
			SOAP	N
8615 Instant Enhanced Charging Collection Function (IeCCF)	R26 SU8 MAS R26 SU8	27 SU5 MAS R27 SU2	Bx	N
			Ga	N
			Rf (Diameter)	N
			Sh	N
			Ro (Diameter)	N
8950 Services Activation Manager (SAM)	On HP platform: R15.5.4	On Sun/Linux platform: R16.0.3 On HP platform: R15.5.5	LDAP	N
			SOAP/XML	N
			SNMP	N
			CORBA	N
ACME Element Management System (EMS)	6.0.0p3	6.0.0p3	SNMP HTTP/HTTPS	N
Billing and Traffic System (BTS)	R6.4.1.0.15	R6.4.1.0.15	AMA/BAF	N
			CDR	N
Enhanced Services Manager (eSM)	R26 SU9	R26 SU9	CORBA	N
			XML/SOAP	N

Product	**Product release for IMS 07.04.00**	**Product release for IMS 07.05.00**	**Supported interface(s)**	**Interface(s) changed** • Y (yes) • N (no) • New (for new products in the IMS architecture)
VitalQIP Dynamic Host Configuration Protocol (DHCP)	R7.1	R7.1	SNMP	N
VitalQIP Domain Name System (DNS)				N
VitalQIP tElephone NUmber Mapping (ENUM) Manager	R1.2	R1.2	SNMP XML/SOAP	N

Ports and Protocols - 1300 Cross-Domain Management Center

Overview

Purpose

The following table provides a listing of the ports and protocols available from the 1300 XMC in the IMS Solution.

1300 XMC

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
Flows between NMC and XMC server for 3GPP Northbound interface							
8081	TCP	SOAP	No	Yes	NMC → XMC	Unidirectional	WSDL interface through specific URL
Flows between XMC server and OMC-P							
8080	TCP	SOAP/ HTTP	No	yes	XMC → OMC-P	Unidirectional	NE discovery
Flows between PC and OMC-P							

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
14000	TCP	RMI	No	Yes	PC → NE	Unidirectional	Client-server communication for NE access

Ports and Protocols - 1310 Operations and Management Console - Provisioning

Overview

Purpose

The following table provides a listing of the ports and protocols available from the 1310 OMC-P in the IMS Solution.

1310 OMC-P

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
22	TCP	SSH	No	Yes	OMC-P ⇆ ALGP/LCP/ MAS User Client/OSS ⇆ OMC-P, OMC-P ⇆OMC-P	Bidirectional	Secure Shell for craft access and SFTP.
8009	TCP	AJP	No	No	OMC-P ⇆ OMC-P	Bidirectional	Internal only. AJP logging

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
8443	TCP	HTTPS	Yes	Yes	OS ⇆ OMC-P	Bidirectional	Secured interface for OMC-P Web API (SOAP/XML API).
9650	TCP	XML	Yes	Yes	1310 OMC-P ⇆ 5450 ISC, 5420 CTS	Bidirectional	5060 ICS, 5420 CTS, 5450 ISC/IRC - destination port for configuration management.
14014	UDP	SNMP	Yes	Yes	PCM→ 1310 OMC-P	Unidirectional	Recommended SNMP trap receiver port for PCM. Default is 14002.
14016	UDP	SNMP	Yes	Yes	MAS → OMC-P	Unidirectional	Default SNMP trap receiver port for MAS.

Notes:

1. The term "ALGP" refers to the "Alcatel-Lucent Gateway Platform", which can be a media gateway (MG), media gateway controller (MGC), or signaling gateway (SG).
2. The "internal HSS" is a unique construct of the ICS configuration.

Ports and Protocols - 1440 Operations and Maintenance Center - Home Location Register

Overview

Purpose

The following table provides a listing of the ports and protocols available from the 1400 OMC-H in the IMS Solution.

1440 OMC-H

Destination Port	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
123	UDP	NTP	No	Yes	OMC-H → NTP server	Unidirectional	Network time of day sync

Ports and Protocols - 5900 Media Resource Function

Overview

Purpose

The following table provides a listing of the ports and protocols available from the 5900 MRF in the IMS Solution.

5900 MRF

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
MRFC							
8444	TCP	HTTPS	No	Yes	Administra -tor → MCDP	Unidirectional	MCDP console
MRFP							
10071	TCP	sip_ thsdb	Yes	No	Internal communi -cation	Bidirectional	ACS internal communication
10073	TCP/UDP	tns	Yes	No	Internal communi -cation	Bidirectional	ACS internal communication

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
780	TCP	sip_ thsdb	Yes	No	Internal communi -cation	Unidirec- tional	ACS internal communication
840	TCP	sip_ thsdb	Yes	No	Internal communi -cation	Bidirectional	ACS internal communication
860	TCP	sip_ thsdb	Yes	No	Internal communi -cation	Bidirectional	ACS internal communication
2301	TCP	hpsmhd	No	No	Internal communi -cation	Bidirectional	rotatelogs
5061	UDP	SIP	No	Yes	AS ⇆ MRF-P	Bidirectional	Signalisation SIP (MRFP)
5432	TCP	postmaster	Yes	No	Internal communi -cation	Bidirectional	ACS internal communication
5560	TCP	tp260dvr	No	No	Internal communi -cation	Bidirectional	ACS internal communication
8080	TCP	muxer	Yes	No	Internal communi -cation	Bidirectional	ACS internal communication
2381	TCP	hpsmhd	No	No	Internal communi -cation	Bidirectional	rotatelogs
8443	TCP	muxer	Yes	No	Internal communi -cation	Bidirectional	ACS internal communication

Ports and Protocols - 7510 Media Gateway

Overview

Purpose

The following table provides a listing of the ports and protocols available from the 7510 MG in the IMS Solution.

7510 MGW

The following table provides a listing of some of the ports and protocols available from the 7510 MGW in the IMS Solutions.

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
64981-64988	UDP	TRACE-ROUTE	No	Yes	7510MGW ⇆ IP network	Bidirectional	Destination ports
64980-64987	UDP	TRACE-ROUTE	No	Yes	7510MGW ⇆ IP network	Bidirectional	source ports
3784	UDP	BFD	No	Yes	7510 MG ⇆ BFD peer (Router)	Bidirectional	Port of BFD control packets.

Destination Port(s)	Protocol	Service	Configurable	Firewall Impacting	Initiator/ Receiver	Flow	Description
3785	UDP	BFD	No	Yes	7510 MG ⇆ BFD peer (Router)	Bidirectional	Port of BFD echo packets.

1300 XMC

System Parameters

System Parameter/ Field/Attribute	Description	Range	Default Value	Notes
XMC server general parameters				
XMC hostname	Hostname is configured on the XMC.	String	None	XMC hostname can only include letters, digits, or dash (-) characters. The first character must be a letter. The hostname must not be set to 'xmc' or 'XMC' Strings. It must be unique in the customer's network.

1440 OMC-H

System Parameters

System Parameter/ Field/Attribute	Description	Range	Default Value	Notes
session_poll_period	The period in minutes to check that the opened user sessions are alive. Requires stop and start of the process to load the new value	10 seconds - 3600 seconds	15 minutes	The value does not have any range but it is advisable to keep a low value as this is related to the heartbeat of the client. A higher value could increase the traffic between the OMC-H and the client.

8650 SDM

System Parameters

SystemParameter/ Field/Attribute	Description	Range Value	Default Value	Notes
Password	HTTP Digest authentication Password data. Only digits and English letters will be allowed.	Type: string Length: 4 to 32	No default	Password. Optional

BTS

System Parameters

System Parameter/ Field/ Attribute	Description	Range	Default Value	Notes
GdiPath	GDI Date path.		./data	
EnableConfig-urableLDC	This parameter identifies what value is for the character 3 of Timing Indicator field in the last LDC record.	0 or 1	0	0 -The character 3 of Timing Indicator field would be 2 or 9 for non-GR or GR last LDC record. (default) 1 - character 3 of Timing Indicator field would be 4 or 5 for non-GR or GR last LDC record.
IMSCallPty CategorModGen	Enables or disables the generation of Calling Party Category module for CTS.	0 - Disable 1 - Enable	0	
IMSCall TypeModGen	Enables or disables the generation of module 616 for the IMS call type.	0 - Disable 1 - Enable	0	
IMSWhole saleIdModGen	Enables or disables the generation of module 198 for the Calling Party and called party Wholesale ID.	0 - Disable 1 - Enable	0	
IMSAccess NetworkId ModGen	Enables or disables the generation of module 198 for the IMS Access Network Information.	0 - Disable 1 - Enable	0	
IMSAOC ModGen	Enables or disables the generation of module 621 for the Advice of Charge.	0 - Disable 1 - Enable	0	

System Parameter/ Field/ Attribute	Description	Range	Default Value	Notes
IMSService InfoMod Gen	Enables or disables the generation of module 198 for the Service Identifier.	0 - Disable 1 - Enable	0	
CGPNMode ForSDSTrig	For AIN SDS triggers, this parameter defines whether the original calling party number in incoming signaling message should be captured in the Originating Number field (Originating NPA and Originating Number) in structure code 625 (and optionally module 164), or the modified calling party number should be captured.	0 - Record original calling party number 1 - Record modified calling party number	0	
ACMTime StampModule Gen	Enables or disables ACM timestamp module generation (Module 621).	0 - Disable 1 - Enable	0	
ACMTime StampModule Cntxt	ACM timestamp module context. The default is set to 90051.		90051	
ASCII FieldSeparator	The default field separator character in the ASCII billing CDR output is the comma. When this parameter is set to 1, a comma will be used as the field separator in the ASCII billing CDR. When it is set to 2, the pipe '|' character will be used instead of the comma.	1 or 2	1	1 - standard comma field separator (default) 2 - alternate pipe field separator.

System Parameter/ Field/ Attribute	Description	Range	Default Value	Notes
IMSCDR FileIntvl	Defines the IMS STATS CDR file interval when the StatsEnable parameter is set to 3. The default is every fiveMinutes. This is for the 5420 CTS only.	5Minutes 15Minutes 30Minutes 1 Hour I Day		
PegReport Header	Specifies whether or not to include a Peg Counts report header.	0 or 1	0	0 - Header is disabled (default) 1 - Include header
BH Granularity	Specifies the granularity of the busy hour calculation.	5Minutes 30Minutes 1 hour	30 Minutes	
ISDN_CCS _Report	Specifies whether or not to generate the ISDN CCS report.	0 - Reporting is disabled 1 - Enable space delimited report 2 - Enable comma delimited report 3 - Enable both reports (default)"	3	
ISDN_CCS _FileIntvl	Defines the interval at which the ISDN CCS report file is created. The default is every hour.	5 Min 15 Min 30 Min 1 Hour I Day	1hour	5Min - 5 minutes 15Min - 15 minutes 30Min - 30 minutes 1Hour - 1 hour 1Day - 1 day

System Parameter/ Field/ Attribute	Description	Range	Default Value	Notes
PRI_CCS_ Report	Specifies whether or not to generate the PRI CCS report.	0 - Reporting is disabled 1 - Enable space delimited report 2 - Enable comma delimited report 3 - Enable both reports (default)	3	
PRI_CCS_ FileIntvl	Defines the interval at which the PRI CCS report file is created.	5 Min 15 Min 30 Min 1 Hour I Day	1 Hour	5Min - 5 minutes 15Min - 15 minutes 30Min - 30 minutes 1Hour - 1 hour 1Day - 1 day
SnmpTrapId	Unique BTS SNMP Trap ID for OSS northbound system to recognize BTS element.		The default is the Switch Prefix name.	
DialedDigits ModuleGen	Dialed Digits Module Generation.	0,1,2,3	0	0 - Disable 1 - Generate Outpulse digits using Module 101 2 - Generate Outpulse digits using Module 621 3 - Generate dialed digits using Module 198

System Parameter/ Field/ Attribute	Description	Range	Default Value	Notes
GdiHoldFor PriBts	This attribute is used along with GDI V2 otherwise not.	0 or 1	0	0-Disable 1-Do not process the primary GDI files locally as this is a secondary BTS. Files will be copied to a primary BTS for processing.
GdiMaxPriM Byte	This attribute is used along with GDI V2 otherwise not. The maximum mega bytes used for primary GDI files.	0-2000	500 MB	
StatsEnable	Enables or disables the Enhanced Database Traffic Statistics.	0 to 3	2	0 - Disable 1 - Enable Enhanced Database Traffic Statistics 2 - Enable TCA or tsaa traffic statistics (default) 3 - Enable for IMS CDR statistics

Acronym List

A

AGCF
Access Gateway Control Function

ATCA
Advanced Telecommunications Computing Architecture

AR
Action Register

B

BTS
Billing and Traffic System

C

CMS
Change Management System

CTS
Converged Telephony Server

CVoIP
Consumer Voice over IP

D

DNS
Domain Name System

E

eSM
enhanced Service Manager

F

FS
Feature Server

G

GUI
Graphical User Interface

H

HSS
Home Subscriber Server

I

ICC
Internal Convergent Charging

IeCCF
Instant enhanced Charging Collection Function

IMS
IP Multimedia System

IRC
IP Resource Control

ISAM
Intelligent Services Access Manager

ISC
IP Session Control

K

KPI
Key Performance Indicators

L

LCP
Lucent Control Platform

LGP
Lawful Gateway Platform

M

MGC
Media Gateway Controller

MGW
Media Gateway

MRF
Media Resource Function

N

NE
Network Element

NLT
Network Level Test

O

OAM
Operations, Administration, Maintenance

OLCS
OnLine Customer Support

OMC-P
Operations and Maintenance Center – Plexus

P

PCM
Personal Communication Manager

PES
PSDN Emulation Service

PSTN
Public Switched Telephony Network

S

SAM
Services Activation Manager

SDM
Subscriber Data Manager

SSC
Subscriber Services Controller

U

ULIS
Unified Lawful Intercept Suite

V

VoIP
Voice over Internet Protocol

X

XMC
Cross-domain Management Center