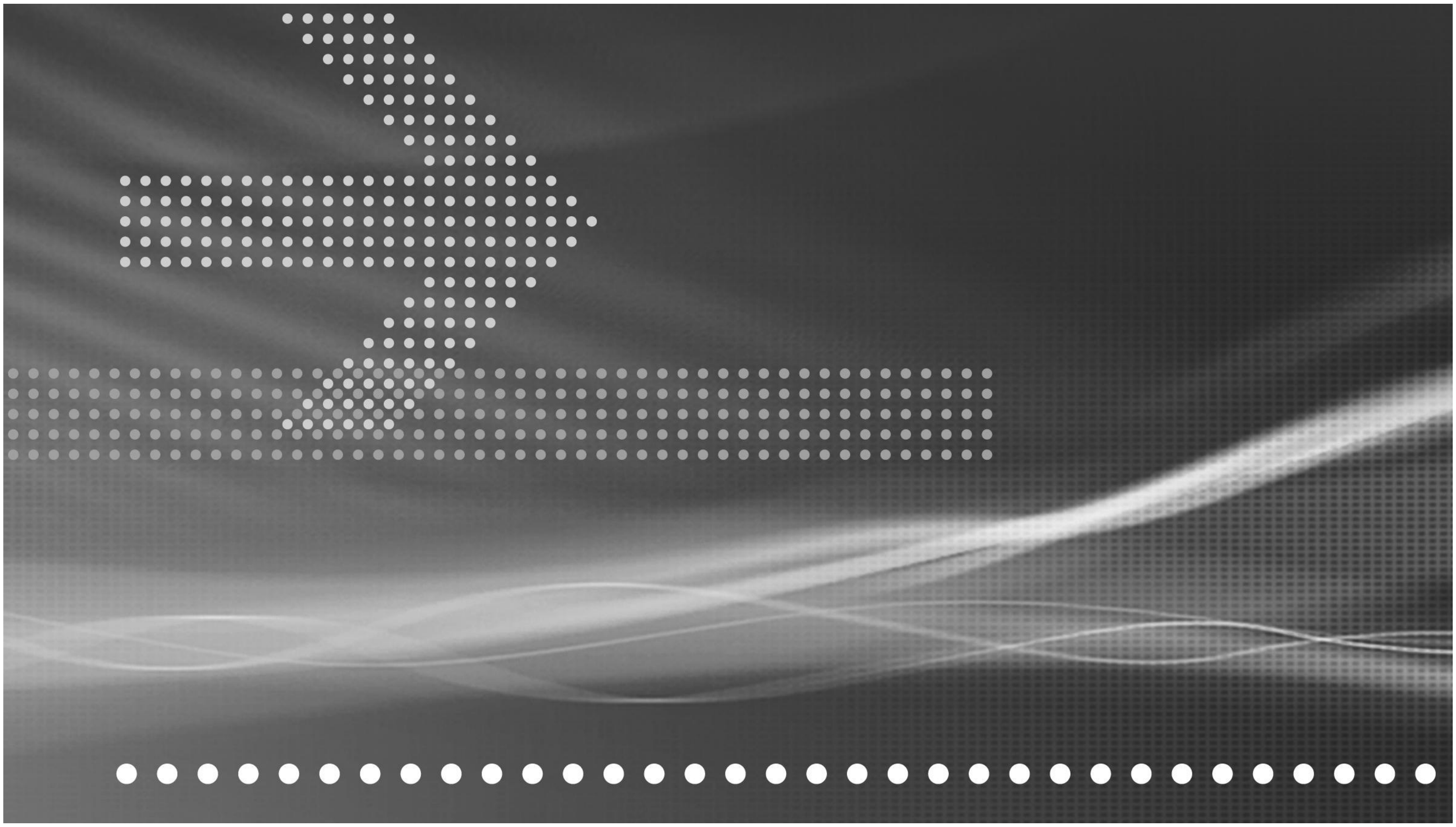


Alcatel-Lucent

IP MULTIMEDIA SUBSYSTEM RELEASE 06.01.18

SOLUTION EXTERNAL RELEASE NOTES

275-100-
004R06.01.18
SEPTEMBER 2009
ISSUE 2

Legal Notice

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Contents

About this document

Purpose

The purpose of this document is to provide a general overview of the IP Multimedia Subsystem (IMS) Release 06.01.18, 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 06.01.18.

Reason for revision

This is the second issue of the IMS Release 06.01.18 Release Notes document. The following table shows the revision history:

Location	Revision	Issue number	Date of issue
Table 2-1	Added feature 33333.354	2.0	September 2009
Table 3-1	Added IP Filtering test results	2.0	September 2009
Table 3-1	Removed feature numbers from first column	2.0	September 2009
Page 3-9	Added paragraph about provisioning throughput tests	2.0	September 2009
Table 6-1	Removed severity 2 MAS-USDS issue (was due to lab config. issue)	2.0	September 2009
Table 6-1	Added new open severity 2 MGC-8 issue	2.0	September 2009
Table 6-1	Added new open severity 2 OMC-P issue	2.0	September 2009
Table 6-2	Added new open severity 2 OMC-P issue	2.0	September 2009
Page 6-2	Changed 07.02.00 to 07.03.00 due to	2.0	September 2009

	release renaming		
Page 8-2	Added information on IP Filtering to Security Hardening section	2.0	September 2009
Appendix A, all pages	Changed all footers to September	2.0	September 2009
Appendix A	Added feature 33333.354	2.0	September 2009

Intended audience

The intended audience for this document includes all personnel who need information about the IMS 06.01.18 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 06.01.18.

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 06.01.18 and the documentation deliverables included in this release.

Software deliverables

Table 1-1 lists the loads that comprise Release 06.01.18. Changes are noted in bold text.

Table 1-1 Software release identification

Network Element/Application	Load Name in IMS 06.01.15b	Load Name in IMS 06.01.18	Load Changed Since IMS 06.01.15b?
2Wire RBGWs[2]	5.29.135.29	5.29.135.29	No
1300 Cross Management Center (XMC)	R6.2.0.3	R6.2.0.3	No
1440 USDS (Includes MAS/AHE)	USDS-04.03.71.18 MAS-R26SU6-p0617 SPA HCF710 SPAHDF710	**USDS_HSS7.1P09** **MAS-R26SU6-p0624** **SPA HCF710** **SPAHDF710** **hlr7.1.p09.01**	**Yes**
5020 MGC-8 (was Lucent Network Controller (LNC), Lucent Signaling Gateway)	6.3.0.4.SP14	**6.3.0.4.SP18**	**Yes**
5020 MGC-12	R2.2.7.13	R2.2.7.13	No
5100 CMS (AnyPath)	AnyPath-R8.2-SU4	AnyPath-R8.2-SU4	No
5350 IMS Application Server (IAS) (Presence, XDMS)	R4.0 SP3.2 + Patches	R4.0 SP3.2 + Patches	No
5440 IMS-PC Client	IMS-PC-Client-R1.3.4-Mtce-v1713	IMS-PC-Client-R1.3.4-Mtce-v1713	No
5450 AGCF	AGCF5_0_0R1S3	AGCF5_0_0R1S3	No
5420 Voice Call Continuity Server (VCC)	SCR 3.1 0R1S1A16 (1.1.1.28)	SCR 3.1 0R1S1A16 (1.1.1.28)	No
5430 Session Resource Broker (SRB)	3.1.1R1P5	3.1.1R1P5	No
5750 Subscriber Services Controller (SSC)	SSCR3.0R1	SSCR3.0R1	No

[2] Please contact 2Wire for software and documentation. Alcatel-Lucent does not warranty this product.

Network Element/Application	Load Name in IMS 06.01.15b	Load Name in IMS 06.01.18	Load Changed Since IMS 06.01.15b?
5900 MRF	6.3.1[3] Required Patches:5990, 6245, 6299, 6360, 6430, 6968, 6976, 7034, 7041, 7591, 7622, 7637, 7881 Previous patches made obsolete by above patches: 6441, 7270 Annlab 4.4.13 MCDP Rel 1.2_Patch12	**6.3.4.4**[4] **Annlab 4.4.13** **MCDP Rel 1.2_Patch12**	**Yes**
7302 ISAM-V	R3.4.01	R3.4.01	No
7302 ISAM-V for Manx[5]	ISAM3.3.02c	ISAM3.3.02c	No
7510 MGW	R2.6	R2.6	No
7520 MGW (was Lucent Network Gateway)	6.3.0.4.SP14	**6.3.0.4.SP18**	**Yes**
7720 Access Border Node (ABN)	R33_04_001-B Reefpoint IQ : IMS 1.2.2.2-QA 29	R33_04_001-B Reefpoint IQ : IMS 1.2.2.2-QA 29	No
8640 Corporate Mobility Manager (CMM)	CMMGEN50-02/05	CMMGEN50-02/05	No
8615 IeCCF (was Surepay CCF)	N440 – eCCF R26SU5-hotslide0103 IeCCF R26SU5-esm-service-hotslide0101 spa ECCF265 MAS R26SU7-p0709 (ltmasr26-p0709) T2000 – IeCCF R27SU3 (Base) IeCCF R27SU3-hotslide0101 spa ECCF268 MAS R27SU2-p0209 (ltmasr27-p0209)	**N440 –** **eCCF R26SU5-hotslide0103** **IeCCF R26SU5-esm-service-hotslide0101** **spa ECCF265** **MAS R26SU7-p0709 (ltmasr26-p0709)** **T2000 –** **IeCCF R27SU3 (Base)** **IeCCF R27SU3-hotslide0101** **spa ECCF268** **MAS R27SU2-p0281 (ltmasr27-p0281)** **G4 v4.2D.0107 NetGuardian T2000 Firmware** **ST6140 RAID Controller fw 06.60.11.10**	**Yes**
8670 GUP (was 1390 GUP)	UPP4.3.1.R1S1P1 ENSUPP4.3.1.R1S1P1	UPP4.3.1.R1S1P1 ENSUPP4.3.1.R1S1P1	No
8680 Video voice Mail Box	3.0.04 patch012	3.0.04 patch012	No

[3] SW 6.3.1 with patches was tested by NLT, but it is recommended that customers wait until 6.3.3 SW is available before applying SW updates**.**

[4] Please refer to the product release notes for upgrade procedures, since there is an OS and BIOS update for this release.

[5] Not part of the generic reference architecture.

Network Element/Application	Load Name in IMS 06.01.15b	Load Name in IMS 06.01.18	Load Changed Since IMS 06.01.15b?
8950 Vital AAA[6]	VitalAAA-5.2.2	VitalAAA-5.2.2	No
Acme Packet Net-Net EMS	EMS 6.0.0p3	**EMS 6.0.0p7**	**Yes**
Acme Packet Session Director (4250)	C5.0.0p24	**C5.0.0p35**	**Yes**
Acme Packet Session Director (9200)	D5.1.0p3	**D6.0.0.m4p5**	**Yes**
Alcatel-Lucent Gateway Platform Software Update Tool	N/A	**V1.6**	**Yes**
Audiocodes – IPM2K	Audio-Codes-IPM1610_SIP_F5.00A.032.003 Audio-Codes for Compact IMS – 5.20A.015.004	Audio-Codes-IPM1610_SIP_F5.00A.032.003 Audio-Codes for Compact IMS – 5.20A.015.004	No
Audiocodes – IPM5K[7]	Audio-Codes-AC_IPM5K_R5.0.50-1.1a	Audio-Codes-AC_IPM5K_R5.0.50-1.1a	No
Dorado[8]	5.3.8.1	5.3.8.1	No
eMRS[9]	eMRS-R25SU9-b0915 (ltcsnr25-b0915) IPMS-255 IPMS-253to255-SPAFU CALEA-251 CALEA-250to251-SPAFU	eMRS-R25SU9-b0915 (ltcsnr25-b0915) IPMS-255 IPMS-253to255-SPAFU CALEA-251 CALEA-250to251-SPAFU	No
eSM	PA-RISC-eSM eSM-01.26.06 P9 Itanium - eSM[10]: eSM-01.26.06 P9	PA-RISC-eSM eSM-01.26.06 P9 Itanium - eSM[11]: eSM-01.26.06 P9	No
5400 Intelligent Services Gateway (ISG)	ISG-08.00.00.05 svc-ISGD-800 svc-FW-800 svc-FWD-800 svc-CDBMON-800 svc-CCSIP-800 svc-ISG-800 MAS-R26SU4-p0423 (ltmasnr26-0423)	ISG-08.00.00.06 svc-ISGD-800 svc-FW-800 svc-FWD-800 svc-CDBMON-800 svc-CCSIP-800 svc-ISG-800 MAS-R26SU4-p0423 (ltmasnr26-0423)	No
Intellivic Client	Intellivic 1.2.0.3000	Intellivic 1.2.0.3000	No

[6] 8950 Vital AAA was part of the WiMAX BU lab environment but not specifically tested by IMS 06.01.18 NLT.
[7] Audiocodes – IPM5K was integration tested with CTS and ISC, but it was not tested by NLT in IMS 06.01.18.
[8] Not part of the generic reference architecture.
[9] Not part of the generic reference architecture. It will only be used in certain existing customer configurations.
[10] Itanium version of eSM is not tested by NLT.
[11] Itanium version of eSM is not tested by NLT.

Network Element/Application	Load Name in IMS 06.01.15b	Load Name in IMS 06.01.18	Load Changed Since IMS 06.01.15b?
Lucent Control Platform (LCP) **Includes:** **- 5420 CTS (was Lucent Feature Server 5000)** **- Lucent Feature Server 2500** **- 5450 ISC (was Lucent Session Manager, LSM)**	R14.28.00.06	**R14.28.01.02**	**Yes**
Lucent Communication Manager (LCM)	6.3.5_GA Red Hat Linux Version 3 update 8	**6.3.5_30** **Red Hat Linux Version 3 update 8** **Kernel – 2.4.21-50.xxxxxx**[12] **NVIDIA-0.62-V1.25**[13]	**Yes**
Lucent Network Gateway for solutions with a Lucent Control Platform-based MGCF	Plexus_WAG-6131.C133.0.0	Plexus_WAG-6131.C133.0.0	No
Lucent Security Management Software (LSMS)	9.1.308	9.1.308	No
Lucent VPN Firewall (LVF)	9.1.308	9.1.308	No
OMC-CN	R3.0 SU5	R3.0 SU5	No
OMC-H	R07.05.01.06.16	R07.05.01.06.16	No
OMC-P	13.0.2.02	**13.0.3.3**	**Yes**
Plexus BTS	6.3.1.0.9 TCA 2.0.0.116	**6.3.1.0.9** **TCA 2.0.0.116** **Solaris 10**	**Yes**
PCTel[14]	PCTel-V2.00.23	PCTel-V2.00.23	No
Riverstone (Lucent Ethernet Router)	For 15100, 200 series R1.5.1.2-N -For 15800 series: R1.5.0.7-SA01 or R1.5.0.8-SA01 -For 3100 series: V9.4.1.6 (for support of trials only)	**For 15100, 200 series R1.5.1.2-N** **-For 15800 series: R1.5.0.7-SA03 or R1.5.0.8-SA01** **-For 3100 series: V9.4.1.6 (for support of trials only)**	**Yes**
SS8 WDDF (Lawful Intercept Gateway)	3.7.1 SU03 3.7.1 SU04	3.7.1 SU03 3.7.1 SU04	No
VCC Light CAMEL Gateway (LCGW)	OSP platform: R2.4.2 + LCGW 1.0	OSP platform: R2.4.2 + LCGW 1.0	No

[12] Please refer to the product release notes to verify/update RedHat OS kernel version prior to upgrade of NE for all LCM nodes.

[13] Please refer to the product release notes to verify/update NVIDIA driver version for NIC card eth0/eth1 prior to upgrade of NE for all X2100 M2 servers.

[14] Trial only

Network Element/Application	Load Name in IMS 06.01.15b	Load Name in IMS 06.01.18	Load Changed Since IMS 06.01.15b?
VitalQIP	VitalQIP R7.1 DNS R4.0 Build 25 ENUM R1.2 VQIP eSM ISR: USDS-04.01.70.06 (only VQIP200 file) Solaris 9 kernel 122300-26 (05/08)	VitalQIP R7.1 DNS R4.0 Build 25 ENUM R1.2 VQIP eSM ISR: USDS-04.01.70.06 (only VQIP200 file) Solaris 9 kernel 122300-26 (05/08)	No
VitalSuite® Services Activation Manager (SAM)	R15.0	R15.0	No
VitalSuite® Voice Activation Manager (VAM)[15]	R13.0, Nov. Patch	R13.0, Nov. Patch	No
Westell TriLink™ Gateway Model 427V A99-427V30a-00	Westell_RBGW-01.00.12.01, sw2.0053.25.01	Westell_RBGW-01.00.12.01, sw2.0053.25.01	No
Windows Mobile Client	WM-Client-PPC-R4.1-V8.0.4.5	WM-Client-PPC-R4.1-V8.0.4.5	No
Zyxel	ZyXEL CPE Rev2 Mother Board MAX210M1_360AKG0b16_20080417 RUNCOM 206.70.24.26 for 3.5ghz or ZyXEL CPE Rev2 Mother Board MAX200M1_360AKG0b16_20080417 RUNCOM 206.70.24.26 for 2.5ghz	ZyXEL CPE Rev2 Mother Board MAX210M1_360AKG0b16_20080417 RUNCOM 206.70.24.26 for 3.5ghz or ZyXEL CPE Rev2 Mother Board MAX200M1_360AKG0b16_20080417 RUNCOM 206.70.24.26 for 2.5ghz	No
Zyxel PCMCIA card (used in PC client)	ZyXEL PCMCIA MAX100_1.0.4.4	ZyXEL PCMCIA MAX100_1.0.4.4	No

How to obtain software

Please contact your Alcatel-Lucent representative to obtain software.

Document deliverables

Table 1-2 shows the solution documentation available for IMS Release 06.01.18.

[15] Not part of the generic reference architecture.

Table 1-2 IMS 06.01.18 solution documentation

Title	Ordering number
*IMS Release 06.01.18 Solution Release Notes**	275-100-004R06.01.18
IMS Release 06.01.18 Interface Changes Specifications	275-100-050R06.01.18
IMS Release 06.01.18 Solution System Parameters	275-100-057R06.01.18
IMS Release 06.01.18 Solution Ports and Protocols	275-100-058R06.01.18

* The *IMS Solution Technical Description* and *Growth* documents are also impacted by 06.01.18 features but are not being reissued for this release. See Appendix A of the *Release Notes* for impacted sections of these documents.

For other solution documents not listed in Table 1-2, please use the latest version (Release 06.01.09).

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.alcatel-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 06.01.18.

New features

The following features are included in this release:

Table 2-1 Features released in 06.01.18

Feature Number	Feature Title
10928.396	Plexus MGW Scripting Enhancement for Plexus R6.3.0.4
33333.118	NLT Testing of Dual FSDB Solution
33333.130	End to End Provisioning Flow Control
33333.134	Synch Phase 2 Solution Testing for CVoIP
33333.138	NLT Testing of CVoIP Growth Module Configuration for 1.848M Subscribers
33333.167	Solution Testing for CVoIP 3.3M Growth
33333.181	Geographic Redundancy Testing for Failure Between Sites of a Module Supporting 1.848M Subscribers
33333.192	Solution Testing for CVoIP 3.3M Growth
33333.225	BTS Solaris Upgrade from Solaris 9 to 10 for Network Assurance Improvements
33333.252	Solution Testing Acme SD 9200 D6.0.0 Load for CVoIP
33333.257	6.1.18 Geo Redundancy
33333.354	Regression Test with IP Filtering enabled on the Plexus MGC/SG/MGW

Functionality

Solution Level support for an additional IMS Core Module of 1.848 Million subscribers was tested in IMS 06.01.18.

Geo-Redundancy testing was completed for MGC12 with the following load combination: MGC12 -Rel.2.1.2 and ISC -Rel 14.25.00.06

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 06.01.18 test program.

Table 3-1 NLT test results

Feature	Test Execution Rate	Pass Rate	
Upgrades	100%	100%	
Regression	100%	99.3%	
Plexus MGW Scripting Enhancement for Plexus R6.3.0.4	100%	100%	
Solution Testing for CVoIP 3.3M Growth (Module 2) - Phase 1	100%	100%	
NLT Testing of Dual FSDB Solution	100%	98.4%	
End to End Provisioning Flow Control	100%	94.3%	
Synch Phase 2 Solution Testing for CVoIP	100%	95.2%	
NLT testing of CVoIP growth module config for 1.848 subs	100%	98.5%	
Geographic Redundancy Testing for failover between sites of a module supporting 1.848M subscribers	100%	91.1%	
Solution Testing for CVoIP 3.3M Growth (Module 2) – Phase 2	100%	100%	
BTS Solaris Upgrade from Solaris 9 to 10 for NA improvements	100%	100%	
Solution Testing Acme SD 9200 D6.0.0 Load for CVoIP	100%	95.6%	
6.1.18 Geo Redundancy for Module 2	100%	94.1%	
Regression Test with IP Filtering enabled on Plexus MGC/SG/MGW	100%	94.4%	
Solution	**Test Execution Rate**	**Pass Rate**	**Exit Criteria Status (Reached/Not Reached)**
IMS Release 06.01.18 Total	100%	97.8%	Reached

See Table 6-1 for Release 06.01.18 exceptions.

Performance test results

The following performance test results are included here:

- Acme 4250
- Acme 9200
- Module 2 Growth
- Site Failover of 924K Subscribers
- End-to-End Provisioning

Acme 4250 Performance Results:

During IMS 06.01.18 NLT, Acme 4250 capacity and registration storm/flood testing was performed. The following tables contain the capacity test results.

The call set-up parameters used for these test results include:

- Number of subscribers	72,000
- Call Rate	1.6 BHCA per sub (40 cps)
- Call Hold Time	150 sec (12000 sessions)
- UE Re-Registration Interval	900 sec

Table 3-2 Acme 4250 performance (with registration flood) test results

Registrations Flood Rate	Duration to Reg Subs	Max. Registered Subscribers	Successful Registrations	Registration Failures	Max. Acme CPU	Max. Acme Load Rate	Trans Timeouts	Regis Retrans Access
80/sec (15min test)	15 min	72,000	528,002	0 (0%)	64.5%	47.20%	0	0

Table 3-3 Acme 4250 performance (with call load) test results

Call Load Rate	Successful calls	Call Failures (%)	Successful Registers	Max. Acme CPU	Max. Acme Load Rate	Trans Timeouts	Retransmissions Access
72K subs @ 1.6 BHCA/sub (40 cps per sub)	87827	1 (0.001%)	612067	86.3	72.7	0	0
36K subs @ 1.6 BHCA/sub (20 cps per sub) (existing call load prior to registration flood)	16898	0 (0%)	288000	88.5	87.2	0	0
36K subs registration flood @ 80 reg/sec	45,082	8 (0.01%)	117801	88.5	87.2	0	1

Acme 9200 Performance Results:

During IMS 06.01.18 NLT, Acme 9200 capacity and registration storm/flood testing was performed. The following tables contain the capacity test results.

The call set-up parameters used for these test results include:

- Number of subscribers	180,000
- Call Rate	1.6 BHCA per sub (80 cps)
- Call Hold Time	150 sec (12000 sessions)
- UE Re-Registration Interval	900 sec

NLT observed that during a registration storm of 180,000 subscribers the Acme 9200 DDOS mechanisms will protect the Acme from the registration storm, and limit the IP messages to Acme processes by dropping packets from untrusted queues.

This behavior protects the Acme processes from going into overload; however it causes the duration for all subscribers to register to increase. NLT observed that the Acme 9200 will support approximately 100-120 subscriber registrations per second, regardless of the rate of registration flood. Issue is non-service impacting because 180K registration flood occurs during an access office Acme recovery from failover; subscribers whose registration is delayed will get service from alternate Acme.

Table 3-4 Acme 9200 performance (with registration flood) test results

Registrations Flood Rate	Duration to Register 180K Subs	Successful Registers	Failed Registers	Max Acme SIP Transport Load	Max. Acme SIP Server Load	Max Acme Core Load	Max Acme MBCD Load	Transaction Timeouts	Register Retrans
120 reg/sec (25min flood test)	31 min	312,934	0	46.1%	79.2%	28.3%	31.1%	68374	1,056,015
200 reg/sec (15min flood test)	33 min	354,471	0	48.7%	89.4%	30.6%	29.8%	225269	2,869,741

Table 3-5 Acme 9200 performance (with call load) test results

Call Load Rate	Successful Calls	Failed Calls	Successful Registers	Failed Registers	Max Acme SIP Transport Load	Max. Acme SIP Server Load	Max Acme Core Load	Max Acme MBCD Load	Trans Timeouts	Register Retrans
180K subs @ 1.6 BHCA/sub (80 cps per sub)	125,187	1449 (1.16 %)*	1,043,873	0	53.8%	21.1%	75.9%	51.6%	0	2
90K subs @ 1.6 BHCA/sub (40 cps per sub) (existing call load prior to registration flood)	60,348	0 (0.0%)	351,110	0	29.3%	12.5%	37.8%	27.2%	0	2320
90K subs registration flood @ 200 reg/sec	-	-	493,939	0	67.9%	80.6%	63.2%	29.3%	0	5184

* Failures resulting from lab environment provisioning issue; issue subsequently resolved.

Performance Results for Module 2 Growth (FID 33333.138)

During the IMS 06.01.18 NLT program, testing was executed to measure the performance for one IMS site to support 1.848M subscribers at 1.6 BHCA per subscriber as described in FID 33333.138. Table 3-6 contains the performance results of the tests that were completed.

The call set-up parameters used to produce these results include:

Number of Subscribers:	1,848,000 (1.60 BHCA per subscriber)
Call Rate:	821 cps (2,880,000 BHCA)
Call Hold Time:	150 sec (123,000 sessions)
Test Duration:	48 hours

Table 3-6 Performance results for 1.848M subscribers at 1.6 BHCA

Network Element	Hardware Description	Capacity (BHCA)	Resulting CPU	Stability through test
Acme 4250	4250	116,800	48%	YES
Acme 9200	9200	288,000	45%	YES
ISC	16-IMS Blades	1,478,400	38%	YES
CTS	14-TAS / 2-FSDB	1,478,400	25%	YES
USDS (HCF)	N440	1,478,400	26%	YES
USDS (HDF)	N1280	2,880,000	10%	YES
IeCCF	T2000	184,800	13%	YES
MGC-8	4 - CM	447,000	43%	YES
MGW	4 - IOM	180,000	N/A	YES
VitalQIP DNS	2-N240	2,880,000	1%	YES
VitalQIP ENUM	2-N240	2,880,000	2%	YES

Performance Results for Site Failover of 924K Subscribers (FID 33333.181)

During the IMS 06.01.18 NLT program, testing was executed to measure the performance results when a primary IMS site, supporting 924K subscribers, fails over to the secondary IMS site, which supports an additional 924k current subscribers, as described in FID 33333.181. Table 3-7 presents the performance results of the site fail over tests that were completed.

Table 3-7 Performance results for failover scenario of IMS site with 924k subscribers

Network Element	Hardware Description	Capacity (BHCA)	Capacity (Subs Failing over)	Resulting CPU	Stability through test
ISC	16-IMS Blades	739,200	462,000	22%	YES
CTS	14-TAS / 2-FSDB	739,200	462,000	14%	YES
USDS (HCF)	N440	739,200	462,000	23%	YES
USDS (HDF)	N1280	1,478,400	924,000	23%	YES
IeCCF	T2000	92,400	57,750	31%	YES
VitalQIP DNS	2-N240	1,478,400	924,000	10%	YES

End-to-End Provisioning Performance Results

The following tables show the results of the IMS 06.01.18 End-to-End Provisioning throughput test program.

Provisioning throughput tests were performed during an alarm flood of 30 alarms per second. It was observed that there was less than 5% impact on the provisioning throughput rate during the alarm flood.

Table 3-8 OMC-P northbound transactions measurements test results

2E Run Description	# of Subs on OMCP	# of Subs on LCM	NB-OMCP Orders/Hr	NB-OMCP Trans/Hr	Lowest LCM CPU Idle	Call Log Base
2 LCM; 1 CTS: 2 pri-FSDB (SIP-SIP background call load)	CTS-2.2M LCM-2.0M	1-750K 2-923K	2954	5909	24% (x2100m2) sec A-node	180M
4 LCM; 2 CTS: 4 pri-FSDB (SIP-SIP background call load)	CTS-2.2M LCM-2.0M	1-750K 2-923K 3-198K 4-151K	4328	8667	77% (x2100m2) sec A-node	180M

Table 3-9 OMC-P southbound LCM transactions measurements test results

E2E Run Description	# of Subs on LCMs	OMCP-LCM Trans/Hr	LCM Add Ave Resp	LCM Mod Ave Resp	LCM Del Ave Resp
2 LCM; 1 CTS: 2 pri-FSDB (SIP-SIP background call load)	1-750K 2-923K	2954	0.43s (m) 0.41s (x)	0.33s (m) 0.20s (x)	0.38s (m) 0.14s (x)
4 LCM; 2 CTS: 4 pri-FSDB (SIP-SIP background call load)	1-750K 2-923K 3-198K 4-151K	4328	0.45s (m) 0.17s (x)	0.38s (m) 0.14s (x)	0.41s (m) 0.09s (x)

Note: (m) designates average LCM response times for a system containing a mix of V20z and X2100 M2 servers, while (x) designates average LCM response time for a system containing only X2100 M2 servers.

Table 3-10 OMC-P southbound CTS transactions measurements test results

E2E Run Description	# of Subs on FSDBs	OMCP-CTS Trans/Hr	CTS Add Ave Resp	CTS Mod Ave Resp	CTS Del Ave Resp
2 LCM; 1 CTS: 2 pri-FSDB (SIP-SIP background call load)	1-462K 2-462K	10829	0.65s	0.41s	0.22s
4 LCM; 2 CTS: 4 pri-FSDB (SIP-SIP background call load)	1-462K 2-462K 3-202K 4-168K	15868	0.69s	0.51s	0.26s

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

The following document describes the alarm changes for the 1440 USDS:

- *USDSR7.1 Patch09 Release Notes*, 270-710-942

  - Appendix 17

Message changes

Please consult the NE-specific documentation for new messages or changes to messages in this release.

Ports

No new ports have been reported for this release.

Protocols

No new protocols have been reported for this release.

System parameters

No new system parameters 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 the NLT-reported problems and software-related customer-reported ARs escalated to NLT, that are resolved in IMS Release 06.01.18.

Table 5-1 NLT-reported problems from previous releases resolved in IMS release 06.01.18

NE	Abstract	Resolution
5420 CTS	During End-to-End provisioning throughput testing, FSDB connection went down spontaneously.	SW fixed, verified in Rel 14.28.01.00
5420 CTS	After Geo-red test -fail back primary site, LCM failed to connect to TAS blade due to missing dns entry for fsimsgroup after lock/unlock of TAS blade.	SW fixed, verified in Rel 14.28.00.08
5420 CTS	During recovery of Geo-Red site failure, FSDB switchover failures experienced during start of Static Sync (unquarantine procedure).	SW fixed, verified in Rel 14.28.00.08
5420 CTS	During a Geo-Red site failure test, dbgw error seen during FSDB Dynamic Sync.	SW fixed, verified in Rel 14.28.01.01
5420 CTS	If the 5420 CTS peer to peer connection is lost during the FSDB Dynamic Sync, the CTS incorrectly indicates "STATIC_RESYNC_DONE" at end of Dynamic Sync.	SW fixed, verified in Rel 14.28.00.08
5450 ISC	During Geo-red site failure testing, it was discovered IMS blades only support 10 CTS TAS blade entries on quarantine list.	SW fixed verified in Rel 14.28.00.08
5900 MRF	MRF 5900 has no mechanism to track patches installed on a server.	SW fixed, verified in MRF 6.3.3
5900 MRF	When restoring system from a Mondo backup, the rescue fails.	SW fixed, verified in MRF 6.3.4.1
5900 MRF	MRFCs become active on both sides. cannot sync Sequoia DB.	SW fixed, verified in MRF 6.3.4
LCM	If more then 8 LCM A-nodes are isolated on single site, the remaining A-nodes JBOSS process is restarted every 18 minutes.	SW fixed, verified in LCM 6.3.5.24

Table 5-2 Customer-reported ARs from previous releases resolved in IMS release 06.01.18

AR	NE	Sev	Short Description
2091550	5420 CTS	3	PMcontrol command taking long time to complete and FS5K MI cannot perform snmpwalk on eMRS
2097426	5420 CTS	2	New FS5K unable to establish diameter connection
2191799	5420 CTS	2	LSS_dbgwDataInconsistency Alarm
2241460	5420 CTS	1	Experiencing SIP 503 failures on all calls
2208324	5420 CTS	2	Calls stopped working on TAS6 group0-000
2247376	5420 CTS	2	ASDA Communication Failure Tracking Ticket
2158287	5420 CTS	3	During Quarantine MOP, tas blade had to be failed-over to sh-1 for click-2-dial and 3-way-call feature to work
2153956	5420 CTS	3	Simultaneous Ring can be activated when no TNs are in the list
2213315	5420 CTS	2	Static Sync did not report Done in R14.28.00.08
2212095	5450 ISC	2	LSM unable to reach Primary MGC after GeoRecovery
2080048	5900 MRF	2	System job is not deleting performance report files after the specified 7 days
2066511	5900 MRF	2	Attempt to reboot MRF-C1 but shutdown never takes place
2115444	5900 MRF	2	5900 MRFC /var file system lacks overload protection
2245098	5900 MRF	2	MRF-C shutdown command kills cluster and does not halt server
2265740	5900 MRF	2	MRF 5900 completely unavailable - active C node is hung
2290391	5900 MRF	2	MRF-C1 is hung
2297963	5900 MRF	2	MRF 5900 AnnLab Application allows directory browsing via web
2157422	Acme 4250	2	Mismatch between the primary and secondary SD radius connection-Standby SD showing READY but the primary SD showing CONNECT_ATTEMPT
2258374	Acme 4250	2	Calls failing with 503 from Acme after rehome test
2104414	Acme 9200	2	CALEA call fails to anchor in the SD; therefore CALEA calls fails due to no voice re-play
2105771	Acme 9200	3	Unable to connect to the SD via SSH
2108322	Acme 9200	2	Unable to receive the CDR from the sd9200 when hostname and NAS-ID is same but port # is different
2110568	Acme 9200	2	Unable to connect to the server due to no session ID
2110614	Acme 9200	2	Seen the following Error in the FreeRadius Server log: Logout entry for port 5060 has wrong ID
2113842	Acme 9200	2	No Voice path for RG behind NAT'ed Address
2116857	Acme 9200	3	Unable to generate 480 no route found when placing a PSTN to SIP call alter the SD's untrusted side cache expired
2117526	Acme 9200	2	ACME9200 power supply failure did not produce expected traps
2121878	Acme 9200	2	Receiving 483-Too many hops when access side is down-correct message is- 404 no route found
2122198	Acme 9200	2	After the SPU crash RG's were not able to register
2122219	Acme 9200	2	Anomalies seen with the SD9200
2160749	Acme 9200	2	One way talk path after flash-hook when one RG is registered in the SD4250 and another RG in SD9200
2167967	Acme 9200	3	During transfer of SW to its image, directory makes SD9200 temporarily non responsive to ssh or telnet connection
2310994	Acme 9200	2	Acme 9200's Taking MIU/SPU Errors
2119130	Acme EMS	2	Sip response map gets misconfigured with save and activate using EMS
1789074	BTS	2	Unable to locate BTS admin guide to creating/managing new users
1819346	BTS	3	BTS allowing reuse of previous passwords
2123958	LCM	3	LCM unexpected A node to A node traffic w/ destination port 6006 during upgrade to 6.3.5 P17
2236908	LCM	2	Critical issues with IR1.7 LCM load; OS patches required
2247763	LCM	2	LCM NIC does not support autoneg off; Nvidia driver needed
2195721	LCM	2	Question about a frequent error messages in LCM log
2123730	LCM	2	LCM upgrade to 6.3.5 has stalled during script execution

AR	NE	Sev	Short Description
1844784	LGP	3	FS5K not sending RFC2833
1990477	LGP	3	MGCs and SGWs are issuing daily – 1593 alarms Protocol Error condition DUPTX and DPURX
2104051	LGP	2	IOM-4 in rolling reboot. Currently set to OOS MA
2118414	LGP	3	Loss of RTP on standing call during GR LNC failover
2184218	LGP	2	SP-B failed with error ”SP-B CPU-A faulted with status – MODULE_ERR_APP_CORE(79)”
2204582	LGP	3	Legitimate stable calls are being dropped by the MGC randomly instead of being updated via the UPDATE sequence
2244891	LGP	3	OMC-P GUI and Switch FEND Selected NEND Sent to be selected on OPERATE LOOPBACK command when not supported in TL1
2269299	LGP	2	MGW has no audio on SIP to PSTN or PSTN to SIP calls
2272128	LGP	3	SS7:ACM was received after an SS7:CGP (Unconditional Call Forward)
2309293	LGP	3	MGW announcements not playing as provisioned for ISUP REL Cause Codes
2363721	LGP	2	OMC-P having difficulties staying connected to LGP with Secure Shell in OMC-P GUI changed from DISABLED to BOTH
1812211	MAS HSS	2	HSS "Password Construction", rqmnt, some rules appear not to be enforced
1812214	MAS HSS	2	HSS "Password Aging", rqmnt, user not prompted for new password
1812221	MAS HSS	3	HSS “Display of last Date and Time” req, doesn’t display as per reqmnt
1816625	MAS HSS	2	HSS "Password Reuse" rqmnt, can't get HISTORY to engage
1927166	MAS HSS	2	Call failures on migrated subscriber while FS5K1 is in quarantine
1952672	MAS HSS	2	HCF2 won't transfer Diameter PPR msg to HCF1 via Diameter Cluster capability
1994506	MAS HSS	2	Need alarm in HCF when Diameter Cluster Peer Capability is lost
2162862	HSS	2	AR to track the inserted 1-second SAR/SAA delay
2000131	HSS	2	Enhancements to track Diameter PPR delivery to LSM
1686501	OMC-P	4	OMC-P IP Filter rules not displaying correctly for ipHdrPrtcl and pfpPrfld fields
1945993	OMC-P	2	OMC-P GUI Passwords displayed as plain text
1972858	OMC-P	2	ALU Specified LCM update transaction for FS5K Migration Fails
2008791	OMC-P	2	GR Install does not accept all ssh keys for added aliases in /etc/hosts
2156067	OMC-P	2	TIME-OUT Delay Seen Between OMC_P and its API (Port 8443)
2168243	OMC-P	3	ALU fix for AR-1941748 not delivered as promised – OMC_P Problems with insertion of point codes still exists
2176773	OMC-P	2	Mismatch subscriber totals between Sub Conf & Sub Party Counts
2256600	OMC-P	3	OMC-P GR enhancements
1784505	Riverstone	3	SNMP-E-SENDTO_Failed:to Dorado IP. Alarms not seen on EMS during Riverstone Sec Hardening
2056948	Riverstone	2	RS-B cannot ping ENA-8 ports 3 & 4
2119871	Riverstone	1	Core experiencing call issues various network elements, showing alarms
2122067	Riverstone	1	Duplicate of AR- 2119871-core experiencing call issues various network elements, showing alarms
2122228	Riverstone	2	Network connectivity issues in core

6 Known issues

Overview

Purpose

This chapter describes NLT-reported issues that remain open in Release 06.01.18.

Known issues and workarounds

This release has no severity 1 issues that were not resolved in the load that are part of 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 6-2 lists severity 2 issues that are targeted for resolution in IMS Release 07.03.00.

Table 6-1 NLT-reported severity 2 open issues from IMS 06.01.18

NE	Abstract	Impact Statement / Workaround
5900 MRF	During upgrade of MRF5900 from 6.3.1 to 6.3.2. Configuration data was not migrated.	SW fix targeted for MRF 7.0.1.
Acme 9200	Initial 200 reg per sec takes >15min for 180K subs on ACME 9200.	Issue is non-service impacting because 180K reg flood occurs during an access office Acme recovery from failover, subscribers whose register is delayed will get service from alternate Acme. There is no plan to fix this exception.
Acme 9200	The gateway unreachable event along with a switchover between active and standby NPUs could lead to a condition where the Network Processor (NP) on the active NPU is not able to process messages.	SW fix available in Acme D6.0.0m5.
LCM	LCM user migration due to quarantine is slower than expected.	SW fix targeted for LCM R6.3.6.
LCM	During quarantine, the quarantine process does not resume after JBOSS process bounces.	A SW fix targeted for LCM R6.3.6. A work around procedure is available to restart the quarantine process.
LCM	2nd LCM not in correct Master/Slave status after 6.3.5.30 upgrade.	SW fix for DBmon failure targeted for LCM R 6.3.6 in IMS7.3. Recovery procedure available.
MAS-USDS	Unexpected alarms on HCF when LSM disconnects from the secondary HCF	Work-around available to manually clear alarm on Site2 HCF. LSM Diameter design changes in R15.36, targeted for IMS7.3, will obsolete this issue.
MGC-8	LGP connections to OMC-P and telnet sessions can become disconnected after a SP switchover, after modifications have been made to LGP system IP addresses.	SW fix targeted for LGP 6.3.0.4.SP20. Recovery procedure available to switchover SP again.
OMC-P	IP Filter Rules displayed on OMC-P are inconsistent with LGP TL1 rtrv-rule-ip after SP switchover.	SW fix targeted for OMC-P 14.2. A work around is available to use the TL1 rtrv-rule-ip command information from the LGP or perform a Synchronize EM with the LGP before viewing IP Filter data on the OMC-P.

Table 6-2 Customer-reported severity 2 ARs remaining open and targeted in IMS 07.03.00

AR	NE	Sev	Short Description	Target NE Load
1838771	5420 CTS	2	FS5K req, criteria D fails	15.36
1848488	5420 CTS	2	LCP FS5K - Sec. Hardening SW fix	15.36
1838933	5450 ISC	2	LCP/LSM does not comply with password construction rules.	15.36

AR	NE	Sev	Short Description	Target NE Load
2096084	5450 ISC	2	Health -a is failing on LSM	15.36
2086583	LCM	2	tcpdump was somehow running on LCM and ran / out of space	6.3.6
2119887	LCM	2	universe portal is failing attempting to retrieve call history records from communication manager, 6:26 am eastern time when it started	6.3.6
2133181	LCM	2	LCM system has stale users on 01 master segment	6.3.6
2151822	LCM	2	LCM does not know when FS5K is unquarantined	6.3.6
2177179	LCM	2	A-node1 DriverManager problem	6.3.6
2199289	LCM	2	LCM System #2 not adding provisioned subs	6.3.6
2219002	LCM	2	LCM Backup failing "DB segment 1 not in desired Master/Slave state"	6.3.6
2236908	LCM	2	Critical security issues with LCM load	6.3.6
1704566	LGP	2	Security scans of the Plexus components continue to have adverse impacts	7.0
1704571	LGP	2	Alarms and procedures needed to identify when and how to recover Plexus systems that are in an unstable state	7.0
1794987	LGP	2	Customer documentation for all open ports in IMS Elements	7.0
1819557	LGP	2	ALU not compliant with requirement	7.0
1819583	LGP	2	ALU not compliant with requirement	7.0
1819685	LGP	2	ALU not compliant with requirement	7.0
1819687	LGP	2	ALU not compliant with requirement	7.0
1819689	LGP	2	ALU not compliant with requirement	7.0
1819694	LGP	2	ALU not compliant with requirement	7.0
1819700	LGP	2	ALU not compliant with requirement	7.0
1819701	LGP	2	ALU not compliant with requirement	7.0
1820076	LGP	2	ALU not compliant with requirement	7.0
1820078	LGP	2	ALU not compliant with requirement	7.0
1820234	LGP	2	ALU not compliant with requirement	7.0
1820240	LGP	2	ALU not compliant with requirement	7.0
1820249	LGP	2	ALU not compliant with requirement	7.0
1820256	LGP	2	ALU not compliant with requirement	7.0
2247600	LGP	2	LGP Security Hardening not maintained during software upgrades	7.0
2103909	OMC-P	2	OMC-P after upgrade R12.0.2.4 defect - not sorting Trunk Groups	14.1
2144748	OMC-P	2	No option to disable Single User Mode after GUI exit or GUI timeout	14.1
2217570	OMC-P	2	OMC-P 13.0.2.2 fails to Alarm under Congestion and Timeouts	14.1
2373745	OMC-P	2	OMC-P GUI Read-Only user can delete database backup files	14.1.1

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

Acme Packet Net-Net EMS	Java 1.5.0_14
OMC-H client	Java 1.5.0_15
OMC-CN client	Java 1.4.2_17
LCM Admin GUI	Java 1.5.0_15
LCP MI GUI	Java 1.5.0_15
XMC GUI	Java 1.5.0_7 and Java 1.4.2_13
5900 MRF MCDP Alarm GUI	Java 1.5.0_16

The 5900 MRF Annlab GUI version 4.4.13 should be installed on a separate PC with Java Web Start version 1.3 and Java 1.5.0_16.

Table 7-2 shows IMS GUIs with no Java installation dependencies.

Table 7-2 IMS GUIs with no Java installation dependencies

OMC-P client	embedded in OMC-P SW load (Java 1.5.0_07)
eSM	uses existing PC Java plug-ins (Java 1.4.x or 1.5.x)
LSMS	uses existing PC Java plug-ins (Java 1.4.x or 1.5.x)
VitalQIP	not applicable

SUN Operating System Patch Level for Non-Integrated Components

Table 7-3 shows the SUN OS patch level for non-integrated components.

Table 7-3 SUN OS system patch level for non-integrated components

Network Element	OS Level
LSMS	Solaris 9 Kernel 122300-26 (0508)
Dorado	Solaris 9 Kernel 122300-26 (0508)
Acme EMS	Solaris 9 Kernel 122300-26 (0508)
VitalQIP Enterprise	Solaris 9 Kernel 122300-26 (0508)
VitalQIP DNS	Solaris 9 Kernel 122300-26 (0508)
OMC-P	Solaris 9 Kernel 122300-26 (0508)
BTS	Solaris 10 Kernel 139555-08 (0509)

Software licensing keys

This section does not apply to this release.   See the specific NE documentation for more information.

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 06.01.15b to IMS 06.01.18. See the *Alcatel-Lucent Internet Protocol Multimedia Subsystem (IMS) Solution 06.01.00 Software Upgrade* document, 275-100-035R06.01.00, 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:

- *Alcatel-Lucent Internet Protocol Multimedia Subsystem (IMS) Solution 06.01.00 Software Upgrade* 275-100-035R06.01.00

Plexus MGW Scripting Enhancement

Feature 10928.396 is new to this release and automates the MGW upgrade for Plexus. This feature reduces significantly the manual effort needed for an upgrade, the upgrade interval, and the risk due to operator error.

LCM NE Upgrade

Please refer to the product release notes when performing the upgrade for this IMS release. There is a RedHat OS kernel update and the NVIDIA driver for the NIC card for all X2100 M2 servers that must be verified and upgraded prior to completing the NE SW upgrade. Please refer to Table 1-1 for the version levels.

5900 MRF NE Upgrade

Please refer to the product release notes when performing the upgrade for this IMS release. There is an OS update and a BIOS update that must be upgraded prior to completing the NE SW upgrade. Please refer to Table 1-1 for the version levels.

Upgrade paths

Upgrade to IMS 06.01.18 is supported from IMS 06.01.15b. Network Elements may require multiple transitions to go from IMS 06.01.15b to IMS 06.01.18; refer to the specific NE documentation for further details.

Security hardening

IP Filtering is a capability on the LGP to explicitly allow or block IP messaging into the LGP. IMS06.01.18 NLT testing was performed with LGP IP Filtering enabled. The IP Filter rules automatically generated by the LGP were used during NLT testing.

Feature activation

Feature activation is done at the NE-level. Please consult with your Alcatel-Lucent customer support team for more information.

Obtaining and installing third-party software

Contact your Alcatel-Lucent customer support team for more information.

A Release 06.01.18 Solution Documentation Impacts

Purpose

This appendix includes the Release 06.01.18-impacted sections of the *IMS Solution Technical Description* document and the *IMS Solution Growth* document.

The following features impact the *Technical Description* document:

- 33333.118 – NLT Testing of Dual FSDB Solution (located on attached pages 1-6 – 1-8)
- 33333.130 – E2E Provisioning Flow Control (located on attached pages 3-5 – 3-7)
- 33333.134 – Synchronized Phase 2 Solution Testing for CVoIP (located on attached pages 8-24 – 8-28)
- 33333.181 – Geographic Redundancy (located on attached pages 8-24 – 8-28)
- 33333.225 – BTS Solaris Upgrade from Solaris 9 to 10 for NA Improvements (located on attached pages 7-23 - 7-33)
- 33333.354 - Regression test with IP Filtering enabled on Plexus MGC/SG/MGW (located on attached pages 7-23 – 7-26)

The following feature impacts the *Growth* document:

- 33333.118 - NLT Testing of Dual FSDB Solution (located on attached pages 1-1 – 1-5)

Alcatel-Lucent IMS reference architecture

Purpose

This topic describes the reference architecture for the Alcatel-Lucent IMS solutions.

IMS layers

The reference architecture follows IMS standards and is divided in the following layers and domains:

- Access and border
- Session control
- Application
- Management and OAM

The layered architecture and the standardized interfaces between the layers and the network elements in the layers, ensures that functionality is clearly divided. The layering allows functions to be developed or added in a layer without requiring development in other layers.

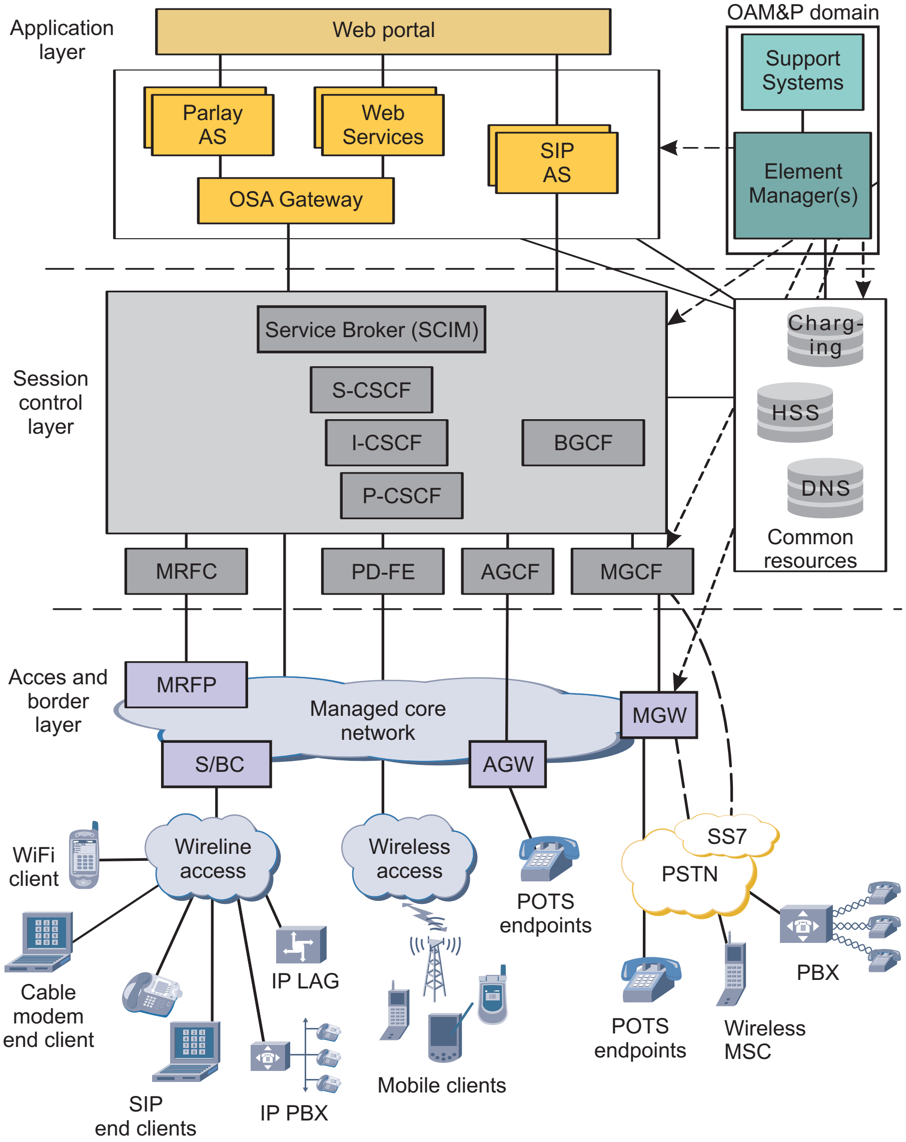
IMS layer functions

The functions of the IMS layers are described in the following table:

IMS layer	Function
Access and border	Provides functions and network elements that offer access to IMS and IMS services.
Session control	Provides functions and network elements to establish sessions.
Application	Provides services to the end user.
Management and OAM	Provides systems for managing the IMS network, the IMS network elements, services, and users.

Reference architecture

The IMS reference architecture is shown in the following figure:



Reference architecture and customer IMS solutions

From the reference architecture, a customized architecture is created for the customer. In the customer IMS architecture products are removed or replaced by alternative products.

Modular growth

With a module, the IMS solution can be built in increments. Modules vary in size depending upon the applications the module is requested to support. The size can support voice subscribers in the 1-3 million range, but this may need to be reduced if applications beyond voice telephony application servers are supported with an IMS core. For more information, see *IP Multimedia Subsystem Growth*, 275-100-059.

□

OMC-P

Purpose

This topic describes the Operation and Maintenance Center - P (OMC-P). The OMC-P is an integrated management center that supports multiple products.

Functions

The OMC-P provides EMS functions and offers FCAPS functionality for the management of southbound network elements.

The OMC-P supports FCAPS functionality:

- Fault management.
  View, filter, acknowledge, synchronize alarms from NEs. Forward fault information to northbound systems. Send SNMP traps to the 1300 XMC.
- Configuration management.
  Navigate through system components and provision network elements. Including inventory management.
- Accounting management.
  Collect and analyze traffic data based on call detail records generated by network elements. This feature requires OMC-P's Advanced Reporting System and Advanced Traffic Collection applications.
- Performance management.
  View performance monitoring, call processing, and operational statistics. Help 1300 XMC to retrieve 3GPP performance management files.
- Security management.
  User authentication and authorization using access control lists and node control lists. Security features are based on Telcordia requirements documents GR-815 and TR835.

The OMC-P supports flow control to enable successful NE provisioning, while blocking or reducing provisioning when the OMC-P is likely to fail. Additionally, excessively delayed queued transactions are failed without consideration to reduce the upstream rollback potential. Effective flow control should be implemented by each northbound NE querying the OMC-P. Effective flow control is required for all NEs provisioning into the OMC-P.

Supported hardware platforms

The OMC-P is supported on the Sun Solaris™ platform hardware.

Supported interfaces

The OMC-P supports the following interfaces:

Interface	between...	and...
TL1 XML SNMP	OMC-P	Southbound network elements
SNMP	OMC-P	Northbound system

Supported northbound systems

The OMC-P supports open northbound interfaces to connect to northbound systems. OMC-P supports XML over the northbound interface for performance management and only supports an SNMP northbound interface to the XMC for fault management.

Supported southbound network elements

The OMC-P OMC-P provides a Java-based client GUI. The OMC-P GUI can be launched from the 1300 XMC client.

The OMC-P supports the following southbound products for fault management, configuration management, performance management, and security management:

- Lucent Control Platform-based products:
  - Lucent Session Manager
  - Lucent Feature Server 5000
- Lucent Network Gateway
- Lucent Network Controller
- Lucent Signaling Gateway
- Lucent Compact Switch
- Lucent Communication Manager
- Lucent MiLife Application Server (fault and performance management)

Charging

The OMC-P does not perform charging functions.

Product documentation

For details on the OMC-P, refer to the following documents:

- *OMC-P for Lucent Gateway Platform Management Reference Guide*, 255-400-400
- *OMC-P for Lucent Control Platform User Guide*, 255-400-420
- *OMC-P for the Lucent Communication Manager*, 255-400-421

□

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
5450 IRC	• No geographic redundancy • Primary - alternate scheme • Load-sharing scheme
5450 ISC	• No geographic redundancy • Primary - alternate scheme • Load-sharing scheme
Alcatel-Lucent Feature Server 2500	• No geographic redundancy • Primary - alternate scheme • Geographic redundancy N+1
5420 CTS	• No geographic redundancy • Primary - alternate scheme • Geographic redundancy N+K • Active-Hot Standby scheme (static sync using peer data)

For more information, refer to *Geographical redundancy* in the *Lucent Control Platform Lucent NC, Lucent SM, Lucent FS 2500 and Lucent FS 5000 - Technical Description*.

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
7520 MGW	No geographic redundancy. The network controller is provisioned with alternate routes and trunk groups to multiple network gateways. In case of network gateway failure, the network controller routes to other network gateways.
5025 VSG	• No geographic redundancy • Hybrid

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.

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)

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

AnyPath® **Messaging System**

The following redundancy schemes can be provisioned for the *AnyPath®* Messaging System:

- Geographic redundancy with load sharing

For more information, refer to *Engineering Guide* of the *AnyPath® Release Documentation*, 270-715-144.

5400 ISG

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

- No geographic redundancy
- Geographic redundancy with load sharing

All SCSs 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 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 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 their database.

For more information, refer to the *SCS User's Guide* of each SCS.

Alcatel-Lucent USDS

The following redundancy schemes can be provisioned for the Alcatel-Lucent Unified Subscriber Data Server (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 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.

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

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.

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 Brick®*s 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.

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

8615 IeCCF

The following redundancy schemes can be provisioned for the 8615 Instant Enhanced Charging Collection Function (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 FS 5000 and Lucent Session Manager share IeCCF. From the FS 5000 and Lucent Session Manager perspective, the IeCCF systems act as primary-alternate systems. In case of failure of a IeCCF, an alternate IeCCF is used.

5350 PS

The following redundancy schemes can be provisioned for the *MiLife*® Presence Solution (PS)

- No geographic redundancy (Simplex Node)
- No geographic redundancy (1+1 redundancy)

AudioCodes® IPMedia media server

The following redundancy schemes can be provisioned for the *AudioCodes*® IPMedia media server:

- No geographic redundancy
- Primary-alternate scheme

In an IMS network, an FS 5000 can be provisioned to use multiple geographically separated media servers. The FS 5000 cycles through each provisioned media server. In case of a media server failure, the FS 5000 accesses the next MRS.

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.

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

5900 MRF

The following redundancy scheme can be provisioned for the 5900 MRF:

- Load-sharing (N+K) scheme

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

□

Security management at the network element level

Purpose

This topic provides an introduction to security management at the network element level.

Security management at the network elements

The individual network elements provide most of the security management services. This is in addition to the security services provided at solution level.

Security management that can be found in network elements include:

- Platform hardening
- Users and passwords
- Role-Based Access Control (RBAC)
- Use of secure protocols (IPSec, SSL, SSH, HTTPS)
- Security logs
- Audits
- IP filtering

Platform hardening

Platform hardening includes the following:

- Disabling of unnecessary network services
- Disabling of unused open ports

Users and passwords

In most IMS network elements, the administrator defines a set of users with access permissions and passwords. The passwords have to comply with a set of rules and can be set, or reset by GUI and CLI interfaces.

The following password complexity rules provide a common set of password strength rules for operations (OAMP) users and do not apply to subscriber passwords. The following rules must be followed when setting or resetting a password and are applicable to both GUI and CLI interfaces unless specified.

- **Password length and characters**
  - The password length must be a minimum of 6 characters and a maximum of 20 characters (default is 6).
  - The minimal number of alphabetic letters required is 0 - 10 (default is 1).
  - The minimal number of special characters required is 0 - 3 (default is 1).
  - The minimal number of numeric digits required is 0 -5 (default is 1).

  - The number of the maximum sequence of characters from the User Id is 0 - 10 (default is 3).
  - The limit for the same characters in a row is 0 - 10 (default is 3).
  - The number of characters allowed in sequence from the previous password is 0 - 3 (default is 3).
  - The password must contain at least one number or special character and must not be in the first or last position.
- **Password strength**
  - The password cannot be the User Id.
  - The password cannot be a reverse of the User Id or a reverse of the previous password.
  - The password settings are case sensitive.
  - The password must not contain a sequence of two or more characters more than once. For example, b94p94.
  - Names, dictionary words or combinations of words should be prevented from being a password in its entirety but can be subcomponents of a password.
  - The time range for a password is from 1 day - 120 days (default is 60).
  - The reuse of passwords is prevented within a settable number of password changes. The range is 0 - 10 (default is 6).
- **Password time limit**
  - When a password is first created or reset, the user has to change the password the first time the user logs in.
  - A password history is supported to ensure that the new password differs from a pre-configured number of previous passwords used by that same user (default history length is 5 and is configurable by the user).
  - The password expiry warning is provided to the user at a provisionable interval of 1 - 10 calendar days (default is 5 calendar days). The warning is provided every time the user logs in prior to the expiration date.
  - The password has to be changed on the login attempt that occurs after the password has expired.
  - The password can be changed at the end of the password aging interval and at the user’s discretion. The interval of the user discretion is subject to a minimal configurable interval of 0 - 24 hours (default is 24 hours).
  - The modifications to password configurable parameters impacts only new passwords from the time of the modification and the passwords constructed against a given rule set remains in effect until the password expires.
- **Password security**
  - The passwords are stored in an encrypted manner.
  - The passwords are sent in a secure encrypted manner.

RBAC

In Role Based Access Control (RBAC), users are assigned to roles. Roles obtain their capabilities from rights profiles and authorizations. Authorizations are generally assigned to the rights profiles with which they are logically associated but can be assigned directly to roles.

A role is a special type of user account from which you can run privileged applications. The capabilities of a role are a function of the rights profiles and authorizations that are assigned to it. When a user assumes a role, the attributes of the role replace all user attributes.

SSH

Secure Shell (SSH) is a software solution for unsafe network commands such as rlogin, rsh, rcp, and telnet. SSH software is not actually a shell, but a protocol that provides an encrypted channel to run a shell on a remote computer.

SSH provides the following functions:

- Authentication of users who log into the network. SSH uses a system of public and private keys and passphrases as digital proof of user identity.
- Data encryption using a variety of encryption methods.
- Data integrity. SSH guarantees that data will arrive at a destination unaltered.

SSL

Secure Sockets Layer (SSL) is a protocol used to secure web-based communications over the Internet at the application layer. It uses encryption and authentication to ensure privacy.

SSL provides the following functions:

- Authentication of users who log into the network. SSL uses a system of public and private keys and passphrases as digital proof of user identity.
- Data encryption using a variety of encryption methods.

HTTPS

HTTPS is Hypertext Transfer Protocol (HTTP) using SSL.

IPSec

IP Security (IPSec), is a suite of protocols that provides security for IP traffic at the network layer.

IPSec provides the following security functions:

- Authentication of the origin of the data. IPSec uses a system of public and private keys as digital proof of origin.
- Data confidentiality. Data is encrypted using a variety of encryption methods.
- Data integrity. IPSec guarantees that data will arrive at a destination unaltered.
- Protection against replay attacks.

Digest authentication

Digest access authentication verifies that both parties to a communication know a shared secret (a password). Unlike Basic authentication, this verification can be done without sending the password in the clear.

Logs

Most network elements maintain a log of system events and user activities. Some maintain a special log for security-related events. These can be used to provide an audit trail to investigate possible security breaches.

Security audits

Some network elements perform periodic security audits. Security audits alert the user about certain security violations on the network element. Any discrepancies discovered by a security audit will generate security alarms.

IP Filtering

IP filtering is used to protect an NE from IP traffic that it has no valid reason to receive. When IP Filtering is enabled, IP Traffic entering the NE is examined and matched against a set of defined IP filters. If the packet matches a filter that allows access to the NE, the packet is passed into the system to be processed. If the IP Packet does not match an IP filter that allows access, the IP packet is discarded.

□

Security management at individual network elements

Purpose

This topic provides an introduction to security management at each individual network element. References are provided for more detailed information.

Security on the Alcatel-Lucent Control Platform

The Alcatel-Lucent Control Platform (Alcatel-Lucent CP) is one of the main components in an IMS network and provides many security management-related services.

Security features on the Alcatel-Lucent CP include:

- Linux platform security hardening features:
  - Disabling of unnecessary network services and unused open ports
  - Message of the day
  - Security audits
  - SSH for external OAM interfaces
  - HTTPS/SSL for OAM&P server, subDB GUI
  - Secure RMI (northbound)
  - Local LDAP server for all intra Lucent CP server login password authentication
- Support for IPSec with Internet Key Exchange (IKE) and anti-replay functionality
- Support for secure Network Time Protocol (NTP)
- Centralized password management
- Role-based access control

For more information, refer to *Lucent Control Platform Lucent NC, Lucent SM, Lucent FS 2500 and Lucent FS 5000 - Technical Description,* 275-900-320.

Security on the 5450 IP Session Control (ISC)

Security features on the 5450 ISC in addition to those provided on the Alcatel-Lucent CP include:

- For the P-CSCF function:
  - The encryption of SIP signaling between the P-CSCF and the UE using IPSec ESP in Transport Mode. The encryption algorithms supported are DES-EDE3-CBC and AES-CBC with 128-bit key.
  - Integrity protection
- For the S-CSCF function:
  - The use of Digest authentication on INVITE requests and REGISTER requests, to reduce the possibility of spoofed calls. Only initial INVITE and REGISTER requests from a UE are challenged.
  - Support for the restriction of users from registering with the IMS network when they are not using their assigned access network (nomadic usage). Nomadic usage is allowed or blocked for a user by data provisioned in the USDS.
  - The generation of security alarms for theft of service. If the S-CSCF receives a failure response to an initial INVITE request, and the INVITE request or failure response contains a non-SDP, non-ISUP message body, then a theft of service security alarm and log are generated.
- For the Service Broker function:
  - A RADIUS interface to access the Central Password management database on the MI agent for password, role, and interface verification
  - Support for HTTPS
- For the Suspended Mode Application Server (SMAS) function, a database of users whose service has been suspended.

For more information, refer to:

- *Lucent Control Platform Lucent NC, Lucent SM, Lucent FS 2500 and Lucent FS 5000 - Technical Description*, 275-900-320
- 3GPP TS 33.203 R6 - Access Security for IP based services
- 3GPP TS 24.229 R6 - IP Multimedia Call Control Protocol based on SIP and SDP

Security on the Alcatel-Lucent Gateway Platform

Security features on the Alcatel-Lucent Gateway Platform (Alcatel-Lucent GP) include:

- Username and password management
- Basic IP filtering - but it is recommended to use a firewall instead
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP) - SNMP version 3 has built-in application-specific security mechanisms that are supported by the switch

For more information, refer to *Lucent Gateway Platform Operations Manual*, 255-400-000.

Security on the Alcatel-Lucent MAS

Security features on the Lucent Milife® Application Server (MAS) include:

- Username and password management
- Support for IPSec
- Support for Secure Shell (SSH)
- Secure Sockets Layer (SSL) encryption of LDAP traffic
- Support for Solaris version of TCP wrappers
- Remote authentication using a RADIUS client
- Disabling of unnecessary network services/open ports
- Security logs

For more information, refer to:

- *Intelligent Network (IN) MiLife® Application Server (MAS) System Description*, 270-710-655
- *Intelligent Network (IN) MiLife® Application Server (MAS) System Administration Guide*, 270-710-167

Security on the Alcatel-Lucent USDS

Security features on the Alcatel-Lucent USDS include authentication of users.

For more information on security management, refer to:

- *USDS architecture Overview* chapter of *Super Distributed Home Location Register (SDHLR) Release 5.0 Product Overview*, 270-710-917
- *USDS Data and Provisioning Guide - ANSI*, 270-710-921

Security on the *AnyPath®* Messaging System

Security features on the *AnyPath®* Messaging System include:

- Username and password management
- Support for Secure Shell (SSH)
- Support for Secure Sockets Layer (SSL)
- Mailbox monitoring and locking
- Security logs

For more information, refer to the *Security* chapter of the AnyPath® *Release 7.0 Documentation*, 270-715-144.

Security on the Alcatel-Lucent VPN Firewall *Brick®* and LSMS

Security features on the Alcatel-Lucent VPN Firewall *Brick*® and Alcatel-Lucent Security Management Server (LSMS) include:

- Username and password management
- Support for IPSec
- Support for Secure Sockets Layer (SSL)
- Logs
- Audits

The primary function of the Lucent VPN Firewall *Brick*® is to provide security. These functions are described in the *Lucent IMS Overview* chapter of this document. The LSMS is an EMS dedicated to the Alcatel-Lucent VPN Firewall *Brick*®.

For more information, refer to:

- *Lucent Security Management Server (LSMS) Technical Overview*, 260-100-011
- *Lucent Security Management Server (LSMS) Administration Guide*, 260-100-005

Security on the *Acme Packet®* Session Border Controller

Security features on the *Acme Packet*® Session Border Controller include:

- Username and password management
- Support for Secure Shell (SSH)
- Overload control
- Session-aware access control for signaling and media
- Topology hiding
- VPN separation
- Session-based authentication
- Security logs
- Audits

For more information, refer to the *Security* chapter of the *Net-Net Session Director Configuration Guide*.

Security on the NexTone iServer™ Session Border Controller

Security features on the NexTone iServer™ Session Border Controller include:

- Username and password management
- Support for Secure Shell (SSH)
- VoIP Firewall
- NAT
- NAT Traversal

- VPN separation
- DoS Protection
- Topology Hiding

For more information, refer to the *Security* chapter of the *Net-Net Session Director Configuration Guide*.

Security on the Alcatel-Lucent Operations and Maintenance Center - H (OMC-H)

Security features on the Operations and Maintenance Center - HLR and HSS (OMC-H) include:

- Support for Secure Shell (SSH)
- Username and password management
- Security logs

For more information, refer to the *Operations and Maintenance Center - HLR and HSS (OMC-H) System Administration*, 401-380-075.

Security on the Alcatel-Lucent Operations and Maintenance Center - P (OMC-P)

Security features on the OMC-P include:

- Support for Secure Shell (SSH)
- Support for Secure Sockets Layer (SSL)
- Username and password management
- Access control lists
- Node access lists
- Security logs

For more information, refer to the following:

- *OMC-P for Lucent Gateway Platform Management Reference Guide*, 55-400-400
- *Lucent Control and Gateway Platform Element Management System (PlexView) Guide for Lucent Communication Manager Applications*, 55-400-421

Security on the eSM

Security features on the Intelligent Network Enhanced Services Manager (eSM) include:

- Username and password management
- Access control
- Logs

For more information, refer to *Intelligent Network (IN) Enhanced Services Manager (ESM) Security Administration*, 270-720-331.

Security on *VitalSuite*® Integrated Service Assurance software

Security features on the *VitalSuite*® Integrated Service Assurance software include:

- Support for IPSec
- Support for Secure Sockets Layer (SSL)
- Username and password management
- Security logs

For more information, refer to the VitalSuite® *Software Integrated Service Assurance and Network Fault Management Administration Guide*, 190-422-820 on the VitalSuite® *ISA Documentation CD-ROM*, 190-422-800.

Security on *VitalQIP*™ DNS/DHCP and ENUM

Security features on the *VitalQIP*™ include:

- Support for Secure Shell (SSH)
- Support for Secure Sockets Layer (SSL)
- Username and password management
- Access control lists
- Node access lists
- Security logs

For more information, refer to the VitalQIP™ *Administrator Reference Manual*, 190-409-042.

Security on *VitalSuite*® Network Performance Management

Security features on the *VitalSuite*® Network Performance Management include:

- Username and password management
- Support for Secure Shell (SSH)
- Support for Secure Sockets Layer (SSL)

For more information, refer to the VitalSuite® *Network Performance Management Software User’s Guide*, 190-409-010.

Security on *VitalSuite*® Software Network Trouble Patterning

Security features on the *VitalSuite*® Software Network Trouble Patterning (NTP) include:

- Username and password management
- Access control lists
- Support for Multi-Protocol Label Switching (MPLS) VPN
- Security logs

For more information, refer to the VitalSuite® *Network Performance Management Software User's Guide*, 190-409-010.

Security on the BTS

Security features on the BTS include:

- Username and password management
- IP Filtering

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

Security on the 5900 MRF

Security features on the 5900 MRF includes username and password management

For more information, refer to *Alcatel-Lucent 5900 MRF Operator Guide*, 3AT34450AAAAGUZZA.

Security on the Alcatel-Lucent CM

Security features on the Alcatel-Lucent CM include:

- Username and password management
- Support for SSL
- Support for SSH

For more information, refer to *Alcatel-Lucent Communication Manager Administration Guide*, 255-490-001.

Security on the Riverstone

Security features on the Riverstone include:

- Username and password management
- Access control lists
- Support for SSH
- Support for SSL

For more information, refer to *Riverstone Networks ES 2010 User Guide*, 36-137-01.

Security on the 8615 IeCCF

Security features on the IeCCF includes username and password management.

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

□

1 Growth overview

Overview

Purpose

This chapter provides an overview of growth in an IP Multimedia Subsystem (IMS) network and describes the methodology and sequence for performing growth for Alcatel-Lucent IMS network elements.

Contents

Growth in an IMS network

Introduction

The Alcatel-Lucent IMS architecture consists of multiple, individual network elements which are integrated together to deliver an IMS solution. Growing capacity of an individual network element can have impacts on other network elements.

When growing a network element, or one of its components, additional provisioning may be required on other elements to use the full growth capabilities.

For example, the growth of a new media gateway control function (MGCF) requires additional provisioning of routers routes on the breakout gateway control function (BGCF) and the growth of a 5420 Converged Telephony Server (5420 CTS) server blade requires provisioning on the Home Subscriber Server (HSS) to allow the server to be used in a subscriber's initial Filter Criteria (iFC).

IMS reference architecture

For the Alcatel-Lucent IMS reference architecture, refer to chapter *Introduction to IP MultiMedia Subsystem, topic Alcatel-Lucent IMS reference architecture* in *IP Multimedia Subsystem Solution Technical Description,* 275-100-000.

Growth information in network element documentation

The network element documentation describes the following growth-related information:

- The types of growth which is allowed for each network element. For example, card, shelf, cabinet, and nodes.
- The engineering rules that must be followed when growing network elements' components.

Growth methodology and sequence

Top down provisioning methodology

The recommended growth methodology is to have a logical progression for growth and to functionally group similar network elements into “buckets”. This logical progression provisions “parent” network elements first and then provision the “children” network elements. The progressions ensure that the data inheritance and data prerequisites are available from the parent to the child network element.

There are two caveats to the top down methodology:

1. The power, cabling, hardware, and other physical installation needed to support the growth is assumed to be a part of the growth procedure and must be completed prior to performing software growth.
2. There are instances, where, after the growth of a child network element, data flows from the child to the parent network element and then from the parent to all the children with the information of the new network element that was grown.

Sequence flow

The recommended growth sequence flow is as follows:

1. Grow the IP network:
   - Alcatel-Lucent VPN Firewall (Brick) / Alcatel-Lucent Security Management Server (SMS) and Fortinet
   - Alcatel-Lucent routers and switches
2. Grow Element Management Systems (EMSs), Network Management Systems (NMSs), Operations Support Systems (OSSs), and other management systems:
   - 1300 Cross-Domain Management Center (XMC)
   - 1300 Convergent Network Management Center (CMC)
   - 1440 OMC - Home Subscriber Server (1440 OMC-H)
   - 8610 Instant Converged Charging
   - 8615 Instant Enhanced Charging Collection Function (IeCCF)
   - Acme Packet ™ Net-Net™ EMS
   - AudioCodes EMS
   - AudioCodes Audio Provisioning Server
   - Billing and Traffic System (BTS)
   - Enhanced Services Manager (eSM)
   - OMC-Plexus (OMC-P)
   - 5620 Services Activation Manager (SAM)
   - 8950 Services Aware Manager (SAM)

3. Grow core databases:
   - 1440 Unified Data Subscriber Server - Home Subscriber Server (1440 USDS - HSS)
   - VitalQIP (including downstream domain name system servers and E.164 tElephone NUmbering Mapping (ENUM) servers.
4. Grow application servers:
   - 5100 Converged Messaging System (CMS)
   - 5400 ATCA IMS Application Server (IAS) applications (5410 Presence Server, 5410 Extensible Markup Language (XML) Document Management Server, and 5430 Multimedia Instant Messaging).
   - 5400 Intelligent Services Gateway (ISG)
   - 5420 Converged Telephony Server (CTS), including Mobility Management Application Server (MMAS) and Hand Off Application Server (HOAS). If the 5420 CTS is co-located with the 5450 IP Session Control (ISC), then it is grown at the same time as the 5450 ISC.
   - 5420 Personal Communication Manager (PCM)
   - 5420 Voice Call Continuity (VCC)
   - Alcatel-Lucent Communication Manager (Alcatel-Lucent CM)
   - Wireless Data Delivery Function (WDDF)
5. Grow the call processing core:
   - 5450 Access Gateway Control Function (AGCF)
   - 5450 ISC
   - 5450 IP Resource Control (IRC)
   - Media Resource Function (MRF) - IPmedia 5000 and 5900 MRF.
6. Grow network interconnect:
   - 5025 Voice Signaling Gateway (VSG)
   - Media gateways - 7510, 7515, and 7520.
   - Media gateway control function (MGCF) - 5020 Media Gateway Controller (MGC) 8, 5060 MGC-10, and 5020 MGC-12.
   - Acme Packet Net-Net Session Director when the Session Director is used as a network interconnect.
7. Grow the access network:
   - 5750 Subscriber Services Controller (SSC)
   - 7302 Intelligent Service Access Manager with Voice package (ISAM-V)
   - Acme Packet Net-Net Session Director when the Session Director is used in the access network.
   - Residential gateway

Modular growth

With a module, the IMS solution can be built in increments. Modules vary in size depending upon the applications the module is requested to support. The size can support voice subscribers in the 1-3 million range, but this may need to be reduced if applications beyond voice telephony application servers are supported with an IMS core.

Acronym List

A

AAA
Authentication, Authorization, Accounting

ABN
Access Border Node

AGCF
Access Gateway Control Function

AGW
Access Gateway

AHE
Application Hosting Environment

AR
Action Register

B

BHCA
Busy Hour Call Attempts

BTS
Billing and Traffic System

C

CALEA
Communications Assistance for Law Enforcement Agency

CCF
Charging Collection Function

CDMA
Code Division Multiple Access

CDR
Call Detail Record

CGF
Charging Gateway Function

CMM
Corporate Mobility Manager

CMS
Change Management System

CPE
Call Processing Equipment

CPS
Calls Per Second

CSCF
Call Session Control Function

CTS
Converged Telephony Server

CUI
Character User Interface

CVoIP
Consumer Voice over IP

D

DNS
Domain Name System

E

E2E
End to End

eCCF
enhanced Charging Collection Function

EMS
Element Management System

ENUM
Telephone Numbering Mapping

eSM
Enhanced Services Manager

ESU
Enhanced Software Upgrade with Scripting

F

FS2500
Feature Server 2500

FS5000
Feature Server 5000 (FS5K) (also known as 5420 CTS)

FSDB
Feature Server Data Base

G

GUI
Graphical User Interface

GUP
Generic User Profile

GPRS
General Packet Radio Service

H

HSS
Home Subscriber Server

I

IAS
IMS Application Server

ICC
Instant Convenient Charging

IeCCF
Instant enhanced Charging Collection Function

IMS
IP Multimedia System

ISC
IP Session Control

ISAM-V
Intelligent Services Access Manager - V

ISDN
Integrated Service Digital Network

ISG
Intelligent Services Gateway

L

LCM
Lucent Communication Manager

LCP
Lucent Control Platform

LIG
Lawful Intercept Gateway

LNC
Lucent Network Controller

LVF
Lucent Virtual private network Firewall

LSM
Lucent Session Manager

LSMS
Lucent Security Management Software

M

MAS
MiLife Application Server

MGC
Media Gateway Controller

MGCF
Media Gateway Control Function

MGW
Media Gateway

MRF
Media Resource Function

N

NA
Network Assurance

NBI
North Bound Interface

NE
Network Element

NLT
Network Level Test

O

OAM
Operations, Administration, Maintenance

OLCS
OnLine Customer Support

OMC-CN
Operations and Maintenance Center – Core Network

OMC-H
Operations and Maintenance Center – Home Location Register and Home Subscriber Service

OMC-P
Operations and Maintenance Center – Plexus

P

PCM
Personal Communication Manager

PNA
Private Network Access

PS
Presence Server

PSTN
Public Switched Telephony Network

PSI
Public Service Identity

S

SAM
Services Activation Manager

SIP
Session Internet Protocol

SMS
Security Management Server

SOAP
Simple Object Access Protocol

SRB
Session Resource Broker

SSC
Subscriber Services Controller

T

TPH
Transactions Per Hour

U

ULIS
Unified Lawful Interception Suite

UMTS
Universal Mobile Telecommunications System

USDS
Unified Subscriber Data System

V

VCC
Voice Call Continuity

VitalAAA
Vital Authentication Authorization Accounting

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

W

WDDF
Wireless Data Delivery Function

X

XMC
Cross-domain Management Center

XML
Extensible Markup Language