Avaya Communication Server 1000
New in this Release

Release 7.6
NN43001-115
Issue 06.02
July 2014

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any

license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

Procedure

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 2: Introduction

This document is a global document. Contact your system supplier or your Avaya representative to verify that the hardware and software described are supported in your area.

Subject

This document contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 (Avaya CS 1000) software. For more information on legacy products and releases, go to http://www.avaya.com/support.

Applicable Systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

In this document, the following terms apply:

- On systems where System Manager is available, the term UCM in the documentation refers to UCM in System Manager. On systems where System Manager is not available, the term UCM in the documentation remains unchanged.
- On systems where System Manager 6.2 is available, the term Subscriber Manager in the documentation refers to User Profile Management in System Manager; on systems where System Manager 6.1 is available, the term Subscriber Manager refers to Subscriber Manager in System Manager; on systems where System Manager is not available, the term Subscriber Manager in the documentation remains unchanged.
- On systems where Session Manager is available, the term NRS in the documentation refers to Session Manager. On systems where Session Manager is not available, the term NRS in the documentation remains unchanged.

Revision history

July 2014	Standard 06.03. This document is up-issued to include a document reference to the new guide *Configuring Routing Service Gateway*.
March 2013	Standard 06.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.6.
April 2012	Standard 05.08. This document is up-issued to remove references to SIP ACD for IVR to support Avaya Communication Server 1000 release 7.5.
August 2011	Standard 05.07. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Changes were made to the IM and Presence application.
August 2011	Standard 05.06. This document is published to support Avaya Communication Server 1000 Release 7.5.
February 2011	Standard 05.05. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Includes new COTS3 server.
November 2010	Standard 05.04. This document is published to support Avaya Communication Server 1000 Release 7.5.

Chapter 3: Overview

Key Attributes

New for CS 1000 Release 7.6

The following sections provide a description of what's new in Avaya Communications Server 1000 (CS 1000) Release 7.6.

Packages

There are no new packages introduced for this release.

Hardware

There are no new hardware updates for Avaya Communication Server 1000 Release 7.6.

Documents

The following documents are retired for Avaya Communication Server 1000 Release 7.6:

- *SIP Trunk Bridge Fundamentals (NN43001–143)*

The following documents are introduced for Avaya Communication Server 1000 Release 7.6:

- *Upgrades Guide (NN43001–408)*
- *Configuring Routing Service Gateway*

Task flows

This section provides high level task flows for the installation or upgrade of a CS 1000 system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the document number that contains the detailed procedures required for the task.

The task flows are also found in *Library Reference, NN43001-100* are in future releases will be the home for the task flows.

This section provides information on the following topics:

Figure 1: Example task flow on page 11 shows an example and how to interpret the task flows.

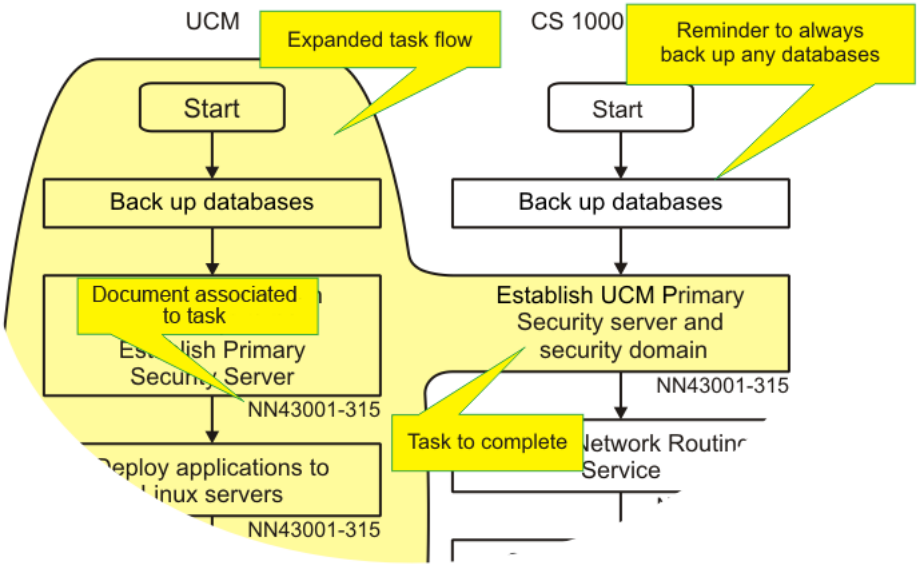

Figure 1: Example task flow

Referenced documents

The following documents are referenced in the task flow diagrams:

- *Planning the Network-wide Upgrade, NN43001-406*
- *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Unified Communications Management Fundamentals , NN3001-116*
- *Network Routing Service Fundamentals, NN43001-130*
- *Communication Server 1000E Installation and Commissioning, NN43041-310*
- *Communication Server 1000E - Software Upgrades, NN43041-458*
- *CP PM Co-resident Call Server and Signaling Server , NN43001-509*
- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning , NN43021-310*
- *CS 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*
- *Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Branch Office Installation and Commissioning , NN43001-314*
- *SIP Line Fundamentals, NN43001-508*
- *Subscriber Manager Fundamentals, NN43001-120*
- *Communication Server 1000E Planning and Engineering – High Scalability Solutions (NN43041-221)*
- *IP Peer Networking Installation and Commissioning , NN43001-313*
- *Communication Server 1000E High Scalability Installation and Commissioning, NN43041-312*
- *Upgrades Guide, NN43001–408*

Network

Figure 2: Network task flow on page 13 appears in *Planning the Network-wide Upgrade, NN43001-406*.

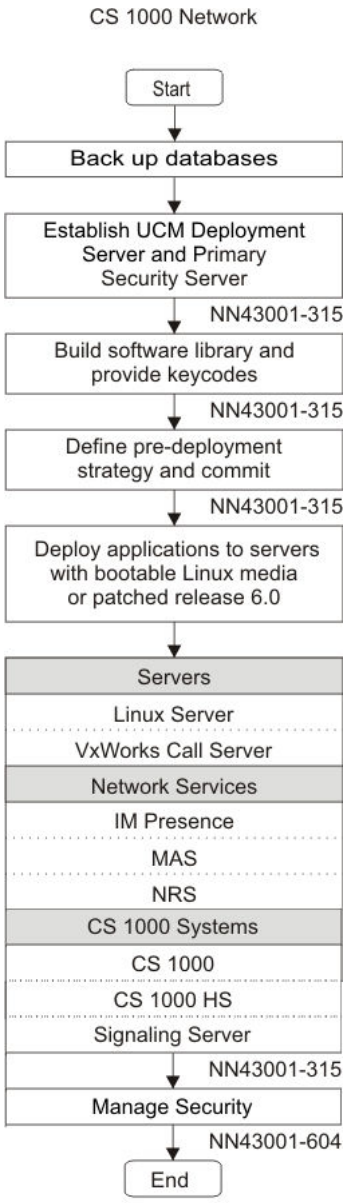

Figure 2: Network task flow

Linux base and UCM

Figure 3: Linux base and UCM task flow on page 14 appears in *Linux Platform Base and Applications Installation and Commissioning, NN43001-315* and *Unified Communications Management Fundamentals , NN3001-116*.

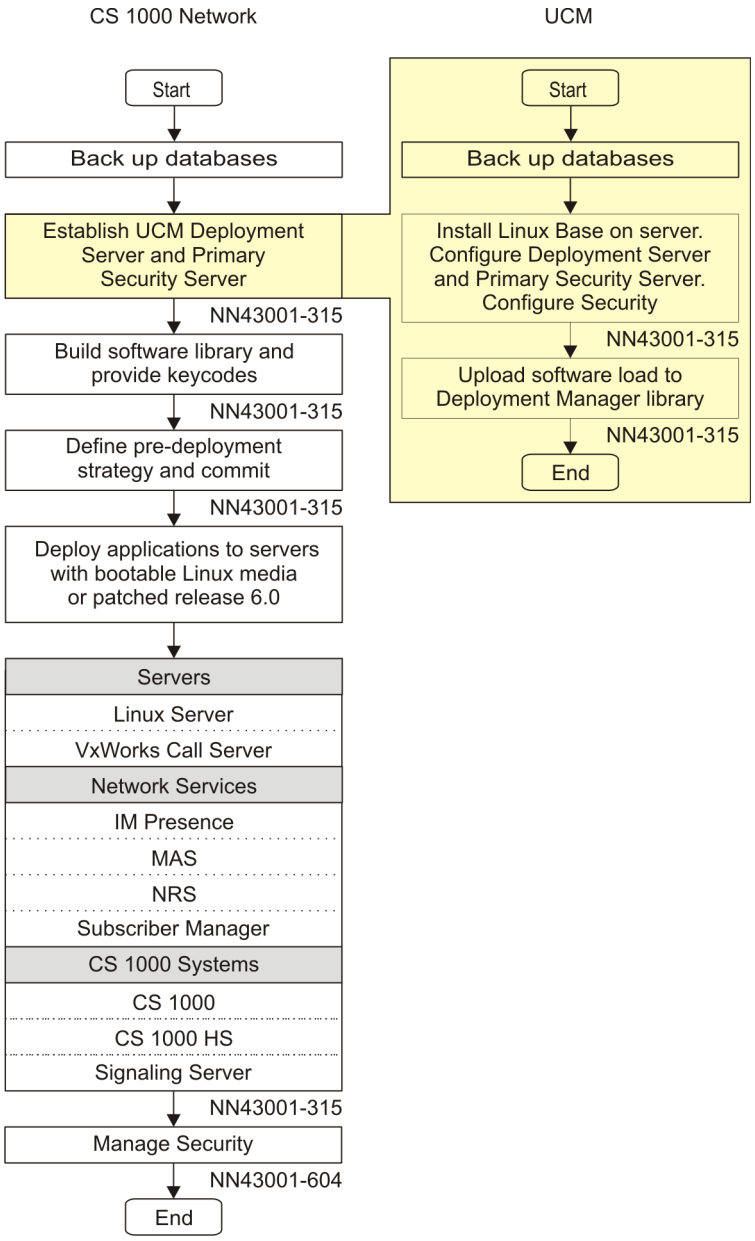

Figure 3: Linux base and UCM task flow

Migration from CS 1000 to Avaya Aura

Figure 4: Migration task flow on page 15, Figure 5: Migration task flow cont on page 16, Figure 6: Migration task flow cont on page 17, andFigure 7: Migration task flow cont on page 18 appear in *Planning the Network-wide Upgrade, NN43001-406*.

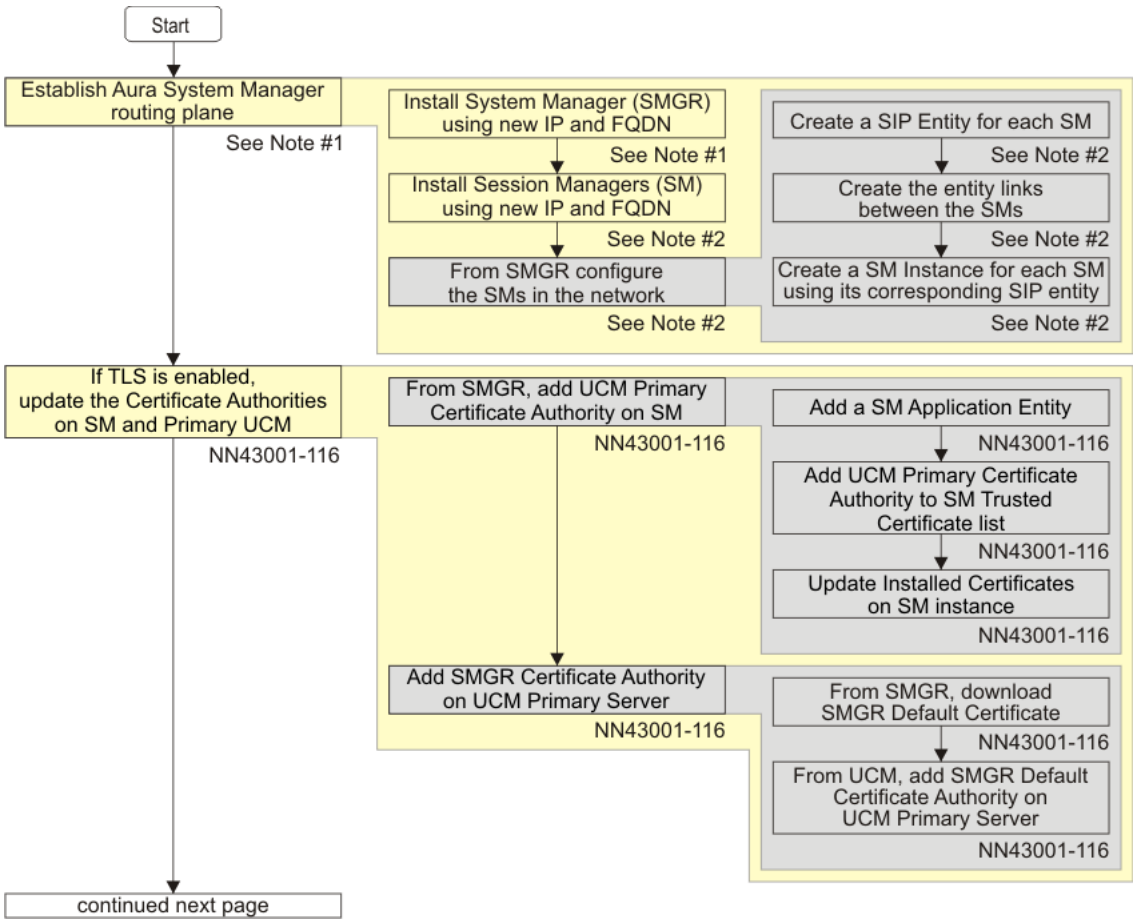

Figure 4: Migration task flow

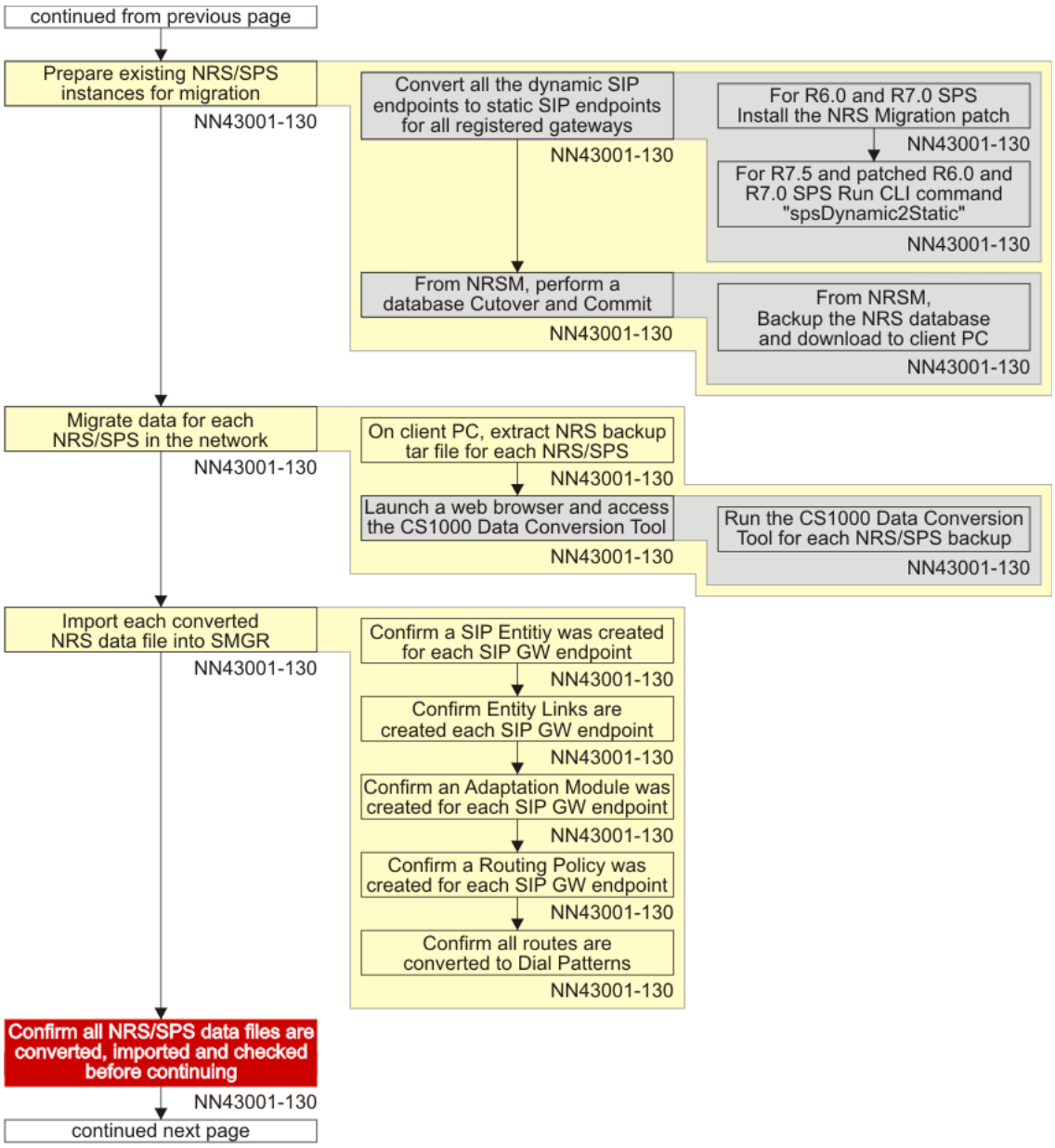

Figure 5: Migration task flow cont

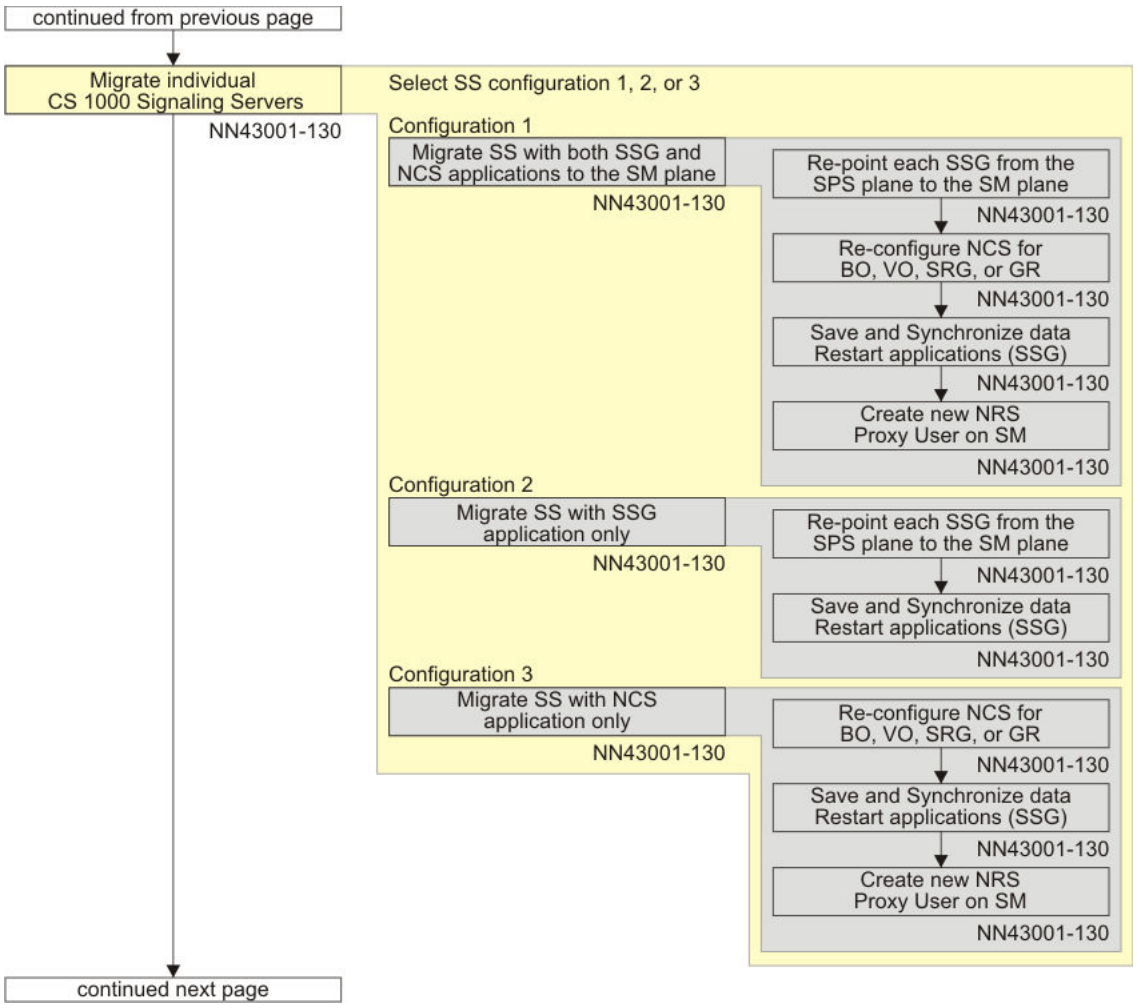

Figure 6: Migration task flow cont

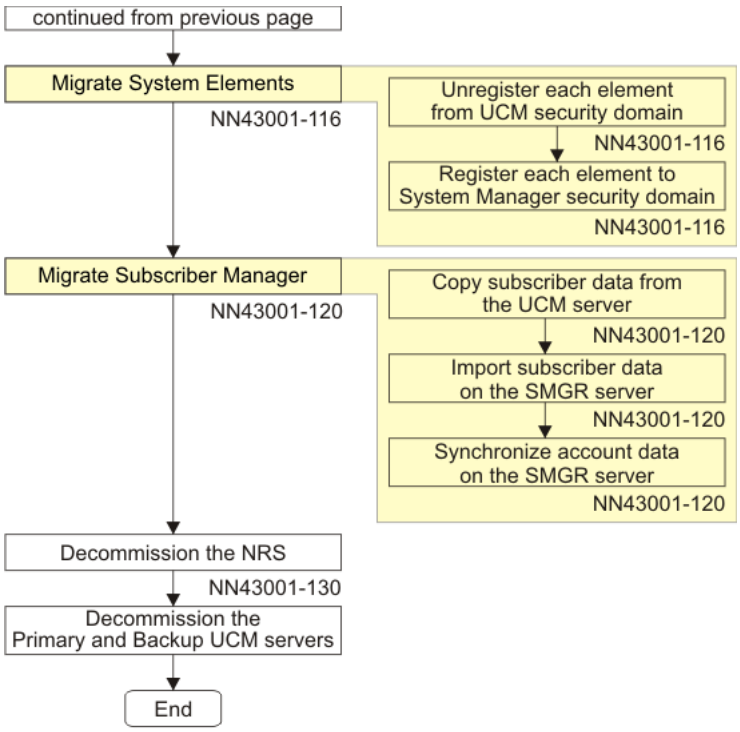

Figure 7: Migration task flow cont

Network Routing Service

Figure 8: Network Routing Service task flow on page 19 appears in *Network Routing Service Fundamentals, NN43001-130*.

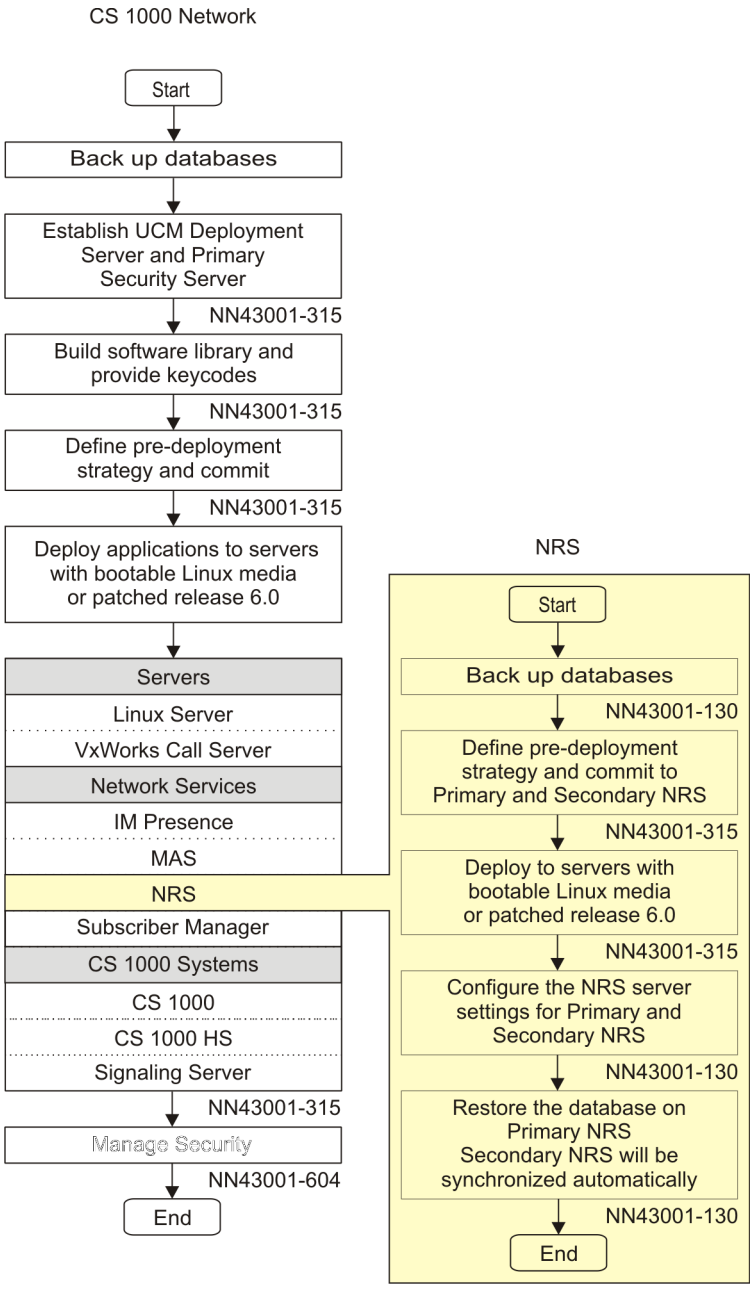

Figure 8: Network Routing Service task flow

CS 1000E High Availability

A CS 1000E High Availability (HA) system can be configured as:

- CS 1000E HA CP IV
- CS 1000E HA CP PM

The CS 1000E HA task flows appear in *Communication Server 1000E Installation and Commissioning, NN43041-310* and *Communication Server 1000E - Software Upgrades, NN43041-458*.

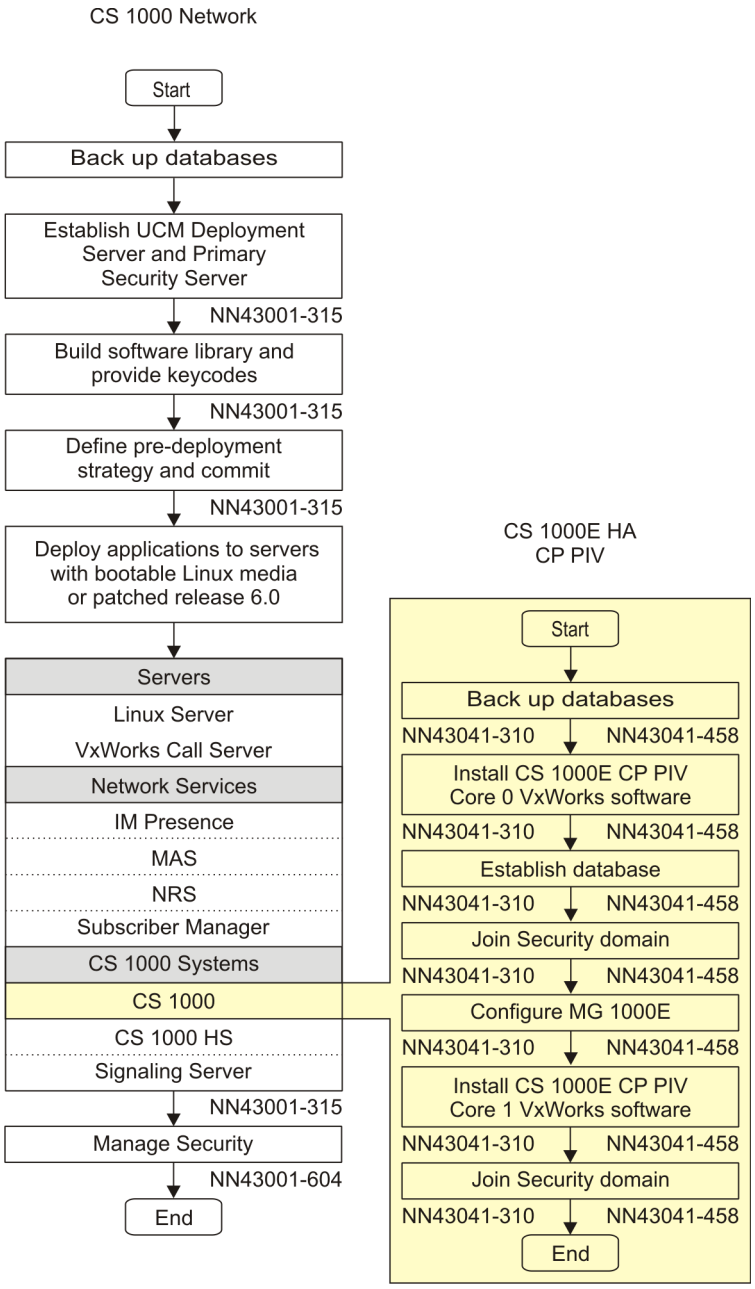

Figure 9: CS 1000E HA CP IV task flow

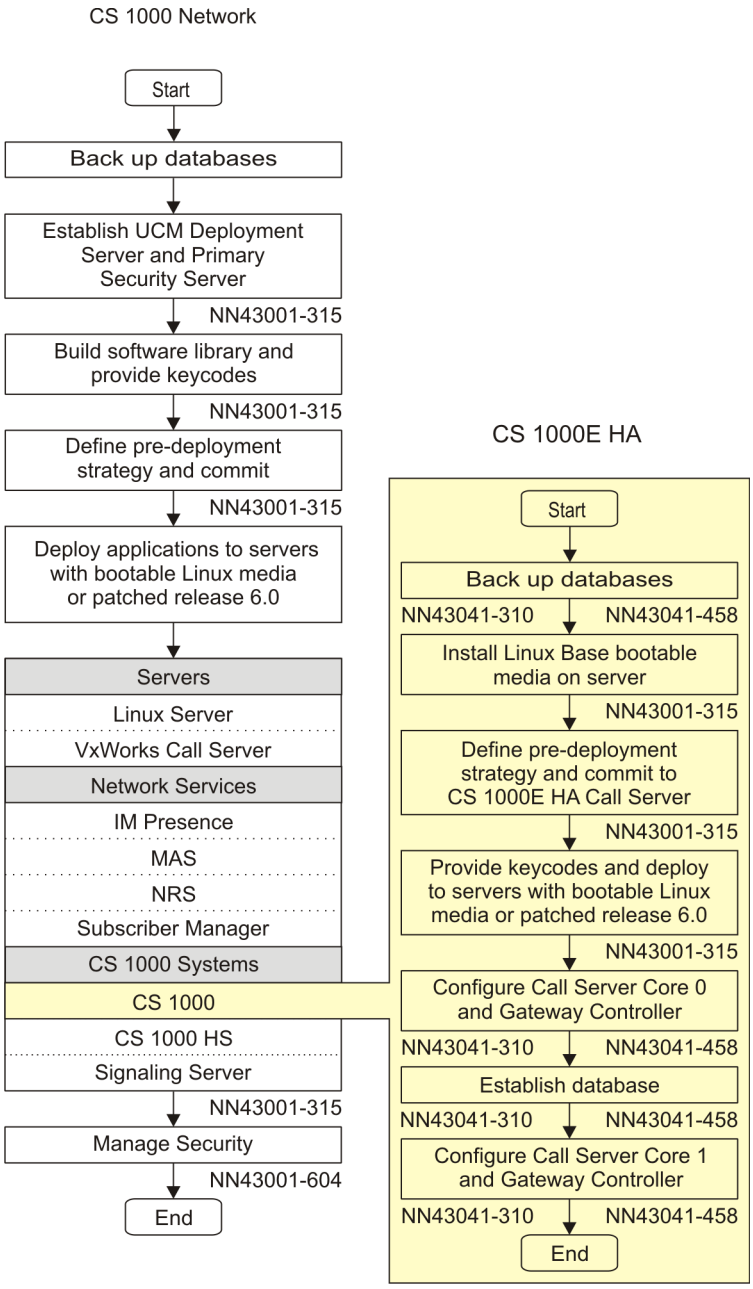

Figure 10: CS 1000E HA CP PM task flow

CS 1000E Co-res

Figure 11: Co-res task flow on page 22 appears in *Co-resident Call Server and Signaling Server , NN43001-509*.

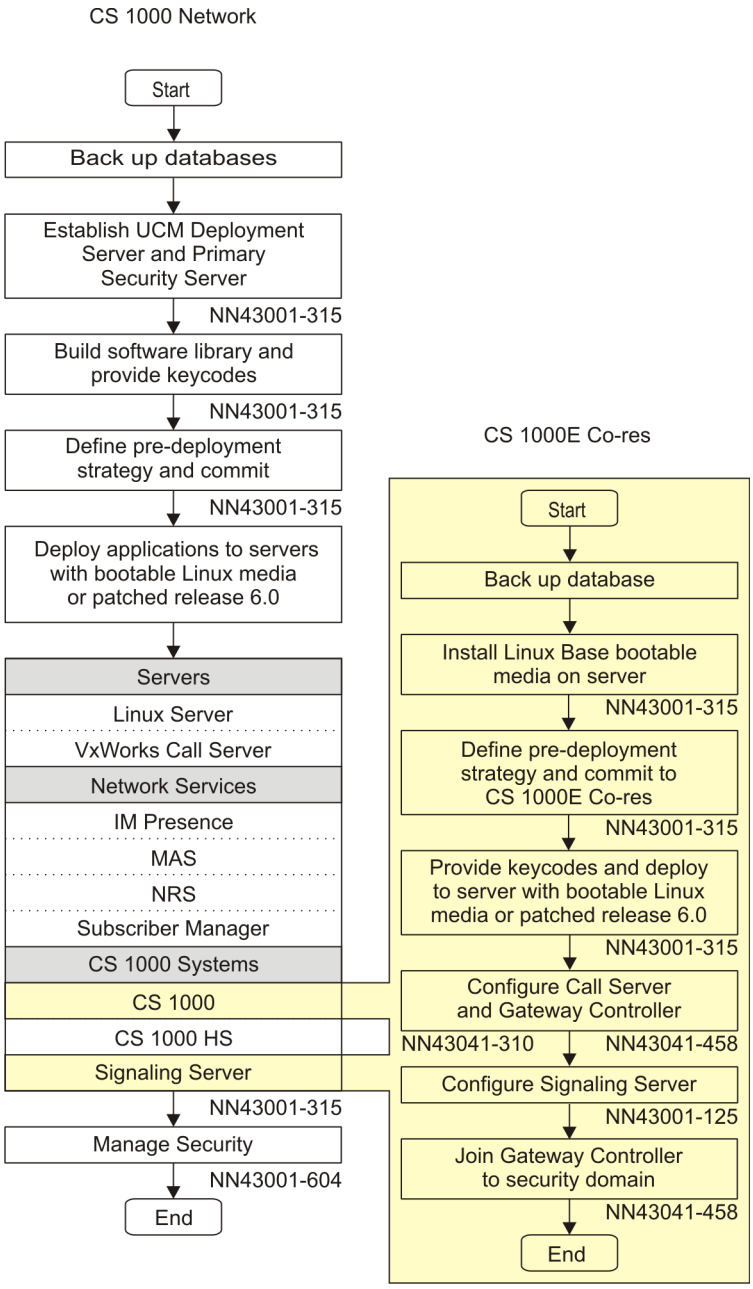

Figure 11: Co-res task flow

CS 1000M

Figure 12: CS 1000M task flow on page 23 appears in *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning , NN43021-310* and *CS 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*.

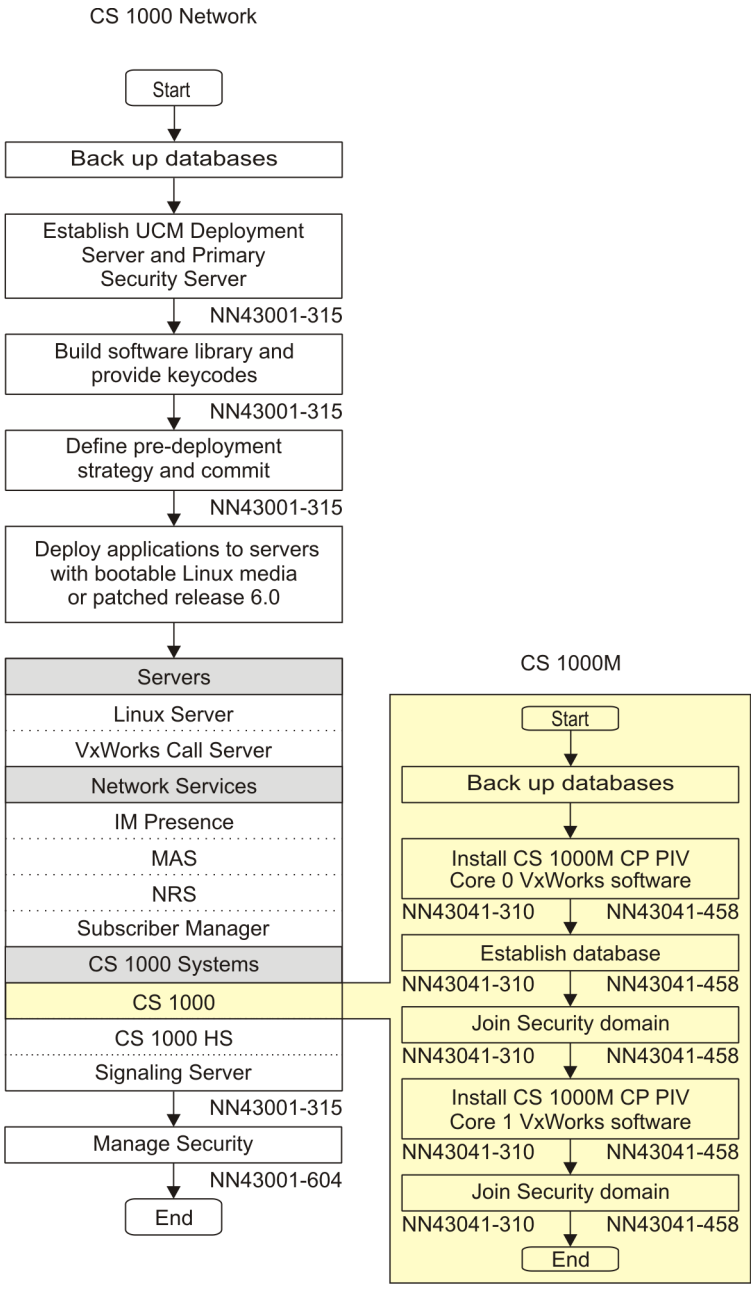

Figure 12: CS 1000M task flow

Signaling Server

Figure 13: Signaling Server task flow on page 24 appears in *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

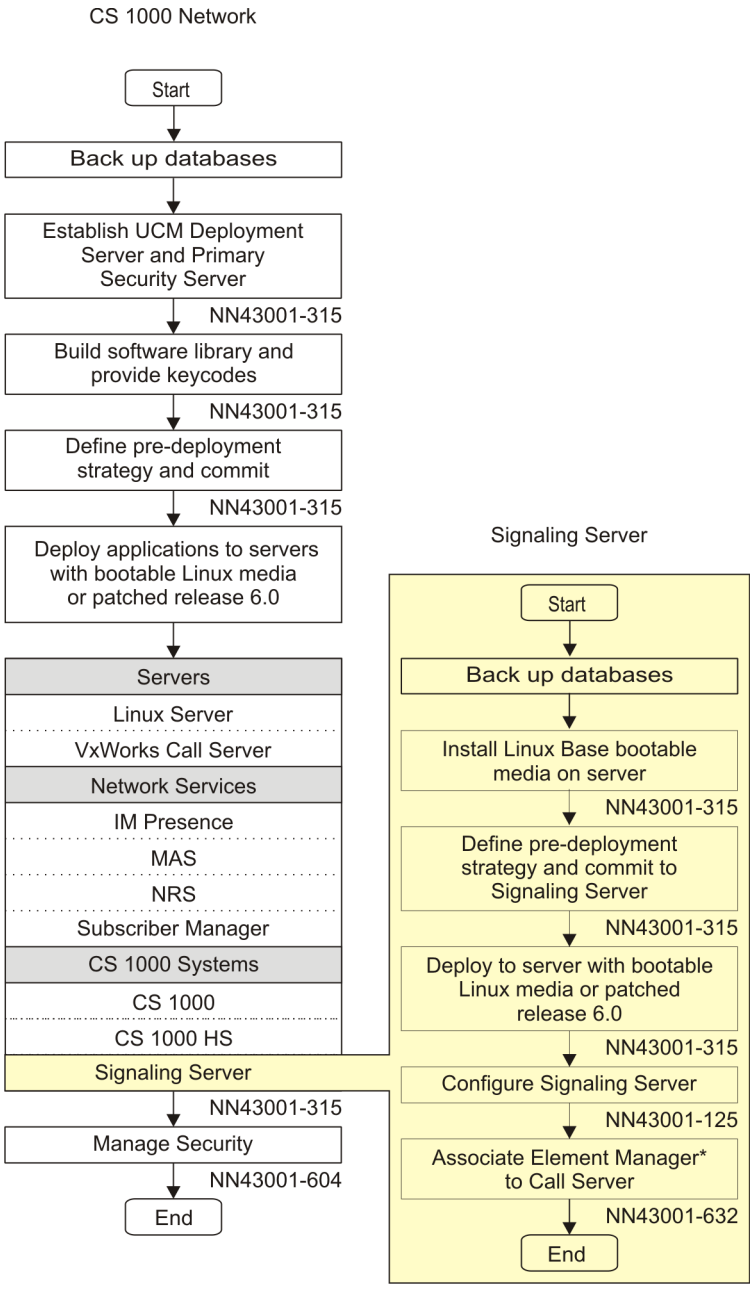

Figure 13: Signaling Server task flow

Branch Office

Figure 14: Branch Office task flow on page 25 appears in *Branch Office Installation and Commissioning , NN43001-314*.

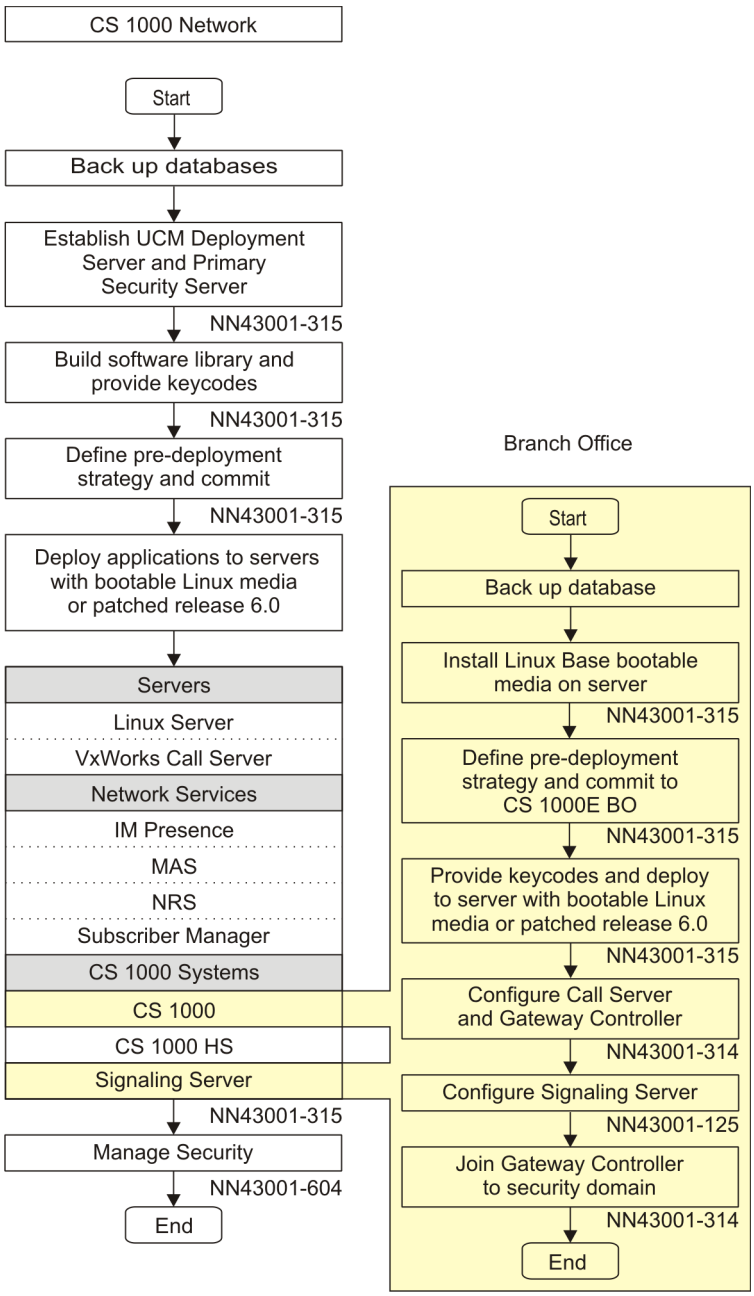

Figure 14: Branch Office task flow

SIP Line

Figure 15: SIP Line task flow on page 26 appears in *SIP Line Fundamentals, NN43001-508*.

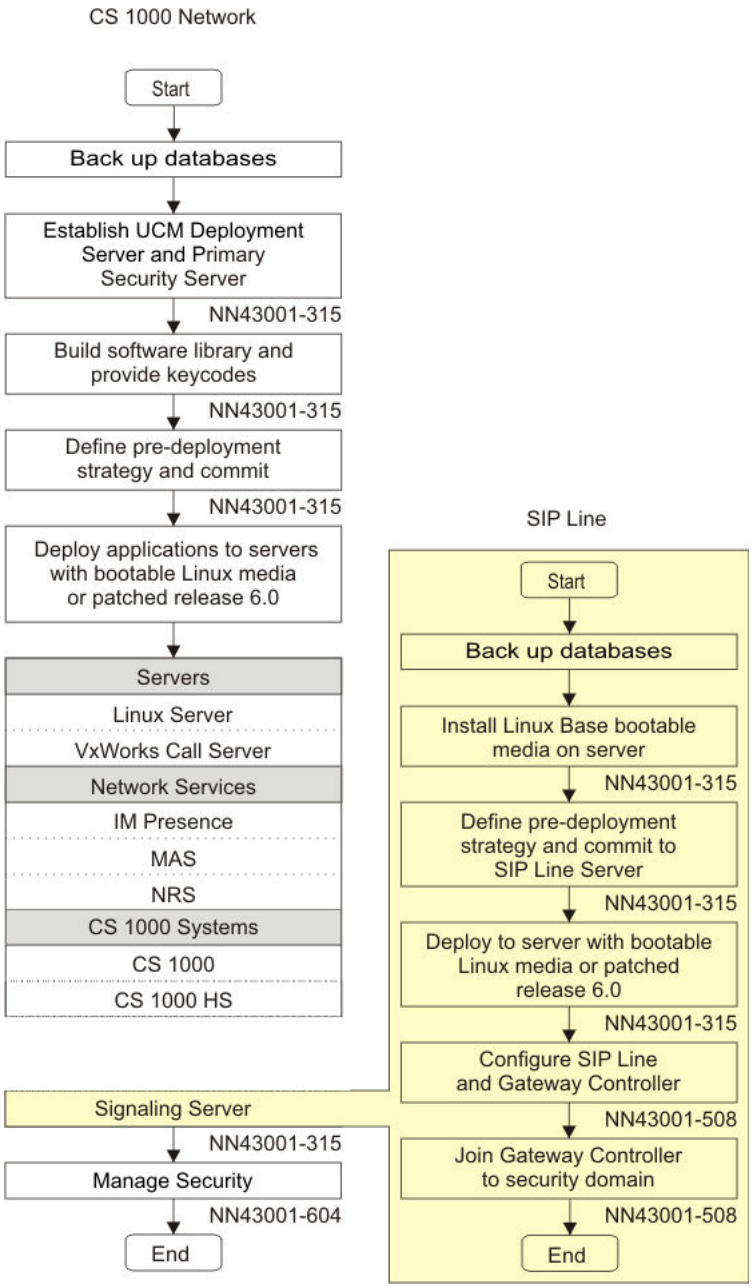

Figure 15: SIP Line task flow

High Scalability

Figure 16: High Scalability task flow on page 27 appears in *Communication Server 1000E Planning and Engineering – High Scalability Solutions (NN43041-221)*.

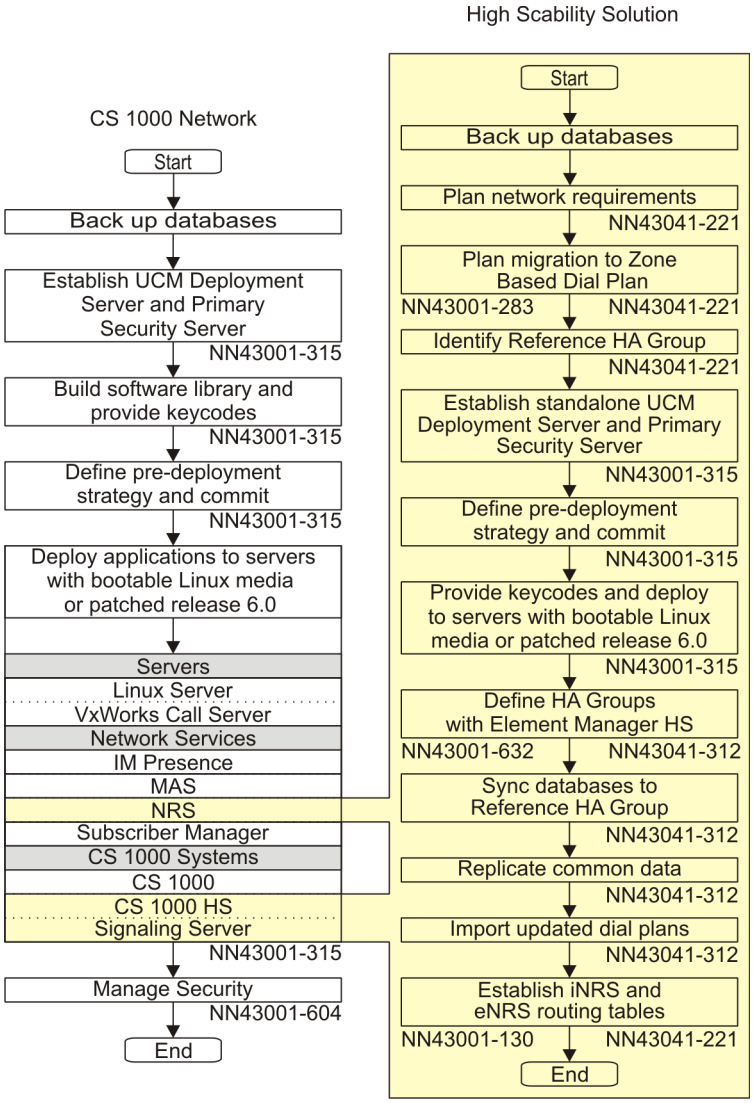

Figure 16: High Scalability task flow

Survivable SIP Media Gateway

Figure 17: Survivable SIP Media Gateway task flow on page 28 appears in *IP Peer Networking Installation and Commissioning , NN43001-313*.

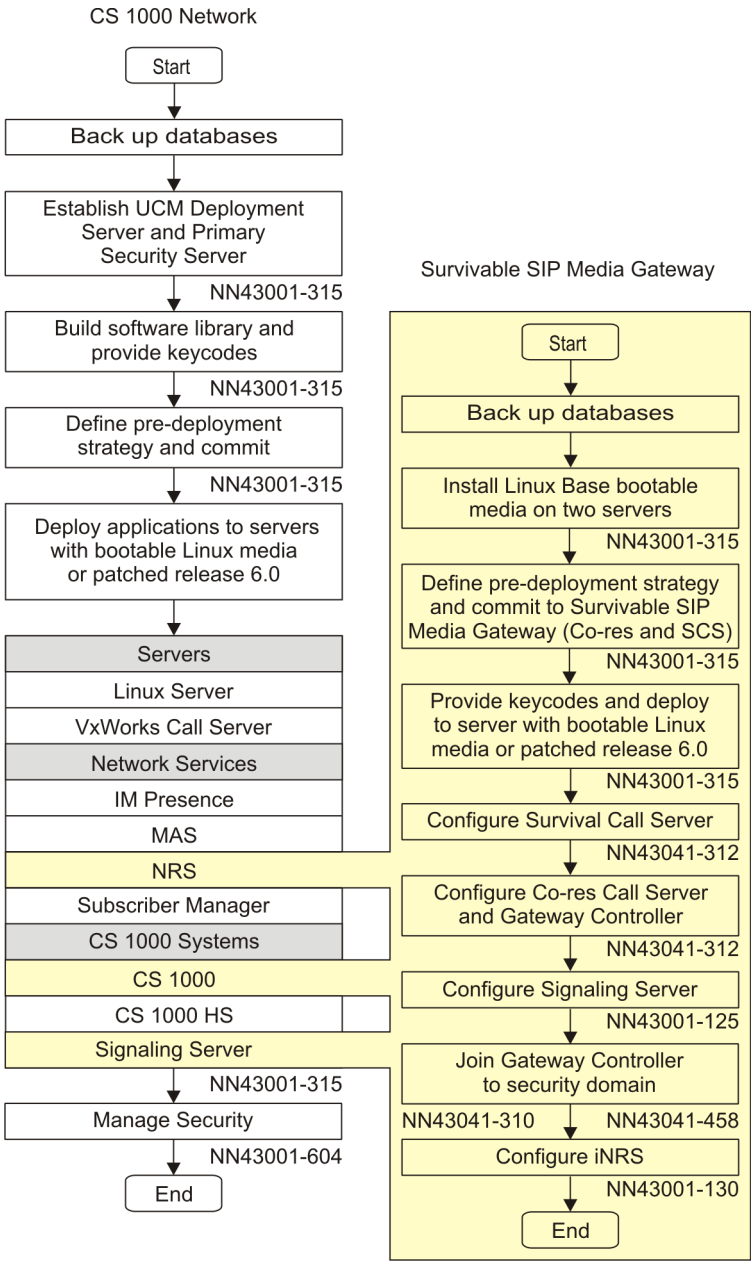

Figure 17: Survivable SIP Media Gateway task flow

Chapter 4: ACD Detailed CDR Call Disconnect indicator

This feature introduces the ability of Call Detail Recording (CDR) blocks configured for ACD agents to indicate whether a call was disconnected by the call originator or by the ACD agent station. When printed, this indicator displays in the third line of the CDR record as either C (caller) or A (agent).

The new ACDD (ACD Detailed) parameter in the Customer Data Block (CDB) configuration for LD 15 can have a value of YES (print the call disconnect indicator) or NO (do not print the call disconnect indicator). The default value is NO.

ACD Package 45 (ACDA) must be unrestricted to use this feature.

For more information, see *Software Input/Output Reference – Administration, NN43001–611*.

Chapter 5: Call Disconnection Tracker

In LD 96, The D-channel Call Trace (DCT) tool has been enhanced to filter incoming and outgoing D-channel messages and to collect additional information about the messages, as follows:

- monitor only messages that have a specified type
- monitor only messages that have a specified cause
- collect Return Address Stack (RAS) and Call Register (CR) information (CRPTR and MSGCR)
- turn on/off these new options
- save RAS and Call Register data in the log file '/e/trace/dct.log'

Messages can be filtered for monitoring by type, cause, or both type and cause.

The Return Address Stack (RAS) option logs RAS information for each message monitored by the DCT tool. The Call Register (CR) option logs Call Register data. CRPTR and/or MSGCR data can also be logged for each message monitored by the DCT tool. The collected RAS and CR data are logged in the new log file **`/e/trace/dct.log`**.

For more information, refer to the chapter **LD 96: D-channel Diagnostics** in *NN43001-711 Software Input Output Reference — Maintenance.*

Chapter 6: DMC DECT Manager Platform Support

Release 7.6 introduces support for two more Windows operating systems for the DMC DECT Manager: Windows Server 2008 and Windows 7.

The DMC DECT Manager provides a point of access and control to manage a DECT system on an Avaya Communication Server 1000 system. DMC DECT Manager runs on the following operating systems:

- Windows 2000 Server
- Windows 2000 Professional
- Windows XP Professional
- Windows Server 2003
- Windows Server 2008 R2 x64/x86 with all available Service Packs and running the same on VmWare
- Windows 7 x64/x86 with all available Service Packs and running the same on VmWare

For information on using DMC DECT Manager, see *Using DMC DECT Manager, NN43001-142*.

Chapter 7: DSP Status Report

A new command ENCT DSP mm is introduced in LD 32 that enables DSP status reports to print on the maintenance terminal. A shortage of DSP resources can be due to units that are disabled, unregistered or busy on active calls. Currently, the Customer traffic report #12 indicates a high peg count for unavailable DSP resources after the fact, at the next scheduled traffic report time.

Traffic reports are not frequently reviewed by support personnel, by printing a DSP utilization summary report periodically on the maintenance terminal this feature allows for better response time in the event of a DSP resource shortage.

To enable the DSP status report, use overlay 32 to enter the command ENCT DSP mm (where mm = number of minutes 15, 30, 60). To disable the DSP status report, enter the command ENCT DSP 0 in overlay 32.

Sample Output:

```
INFO0002 LD32 ECNT DSP IDLE:xxBUSY:yyOOS:zzhh:mm:ssdd/mm/yyyy.
```

This feature is included in base system software.

For more information, see “**DSP Status Report**” in *Communication Server 1000E Software Input Output Reference, NN43001-711*.

Chapter 8: Flexible Calling Line ID

Two of the Flexible Calling Line ID parameters in LD 86, Matching Initial Digits (MID) and Insert Initial Digits (INST), have been increased to support up to 16 digits. This feature is included in base system software.

For more information, see “**Flexible Calling Line ID**” in *Features and Services Fundamentals-Book 6, NN43001-106-B3.*

Chapter 9: Flexible CLID manipulation table enhancements

Communication Server 1000 Release 7.6 introduces the ability of Original Called Numbers (OCN) Matching Number types (MNUM) to use the existing Flexible Calling Line Identification (CLID) manipulation table, which previously only worked for Calling Number (CLNG) MNUM types.

With this enhancement, LD 86 now prints an MNUM type of OCN, the OCN changes in the outgoing or incoming Information Element (IE) in accordance with matched CLID table rules during certain call scenarios, and the Flexible CLID feature corrects the outgoing Route List Index (RLI) of Digital Private Network Signaling System (DPNSS) and Digital Access Signaling System (DASS) calling numbers.

This feature is supported for incoming route or outgoing RLI of UIPE, non-UIPE and DPNSS originally called numbers. For network Call Forward No Answer (CFNA), Call Forward Busy (CFB), and Call Forward All Calls (CFAC) calls, the third-party displays a modified OCN in accordance with the Flexible CLID manipulation table.

In addition, the maximum sizes of the MID and INST fields in the CMDB configuration are now extended from 8 to 16 digits.

For more information about the Flexible CLID manipulation table, see *Avaya Features and Services Fundamentals — Book 3 of 6 (D to H), NN43001-106*.

Chapter 10: Health Check Tool

The Health Check (HC) tool is introduced to provide status information, including a health rating score for different elements of the Avaya Communication Server 1000 system. This information can be used to guide service personnel to the areas of the system that require maintenance or further diagnostics.

Health Check is a PC based GUI application available for download from the Avaya Support portal. It is configured by the user to identify the functionality and network address of the components to be monitored. Once configured, Health Check connects to CS 1000 components including the Call Server, Signaling Server, Media Gateway Controller and Media Cards, via an SSH port through the ELAN connection of each component. Upon connection and based on the functionality of the component, the application issues a set of commands and status requests, and records the results. A pre-defined set of commands is used so the information gathered is interpreted and handled in a controlled way. When the testing of each component is complete, an html report providing an executive level summary of the components is generated and can be viewed from the PC browser.

For more information on the Health Check tool, see *NN43001–408, Upgrades Guide*.

Chapter 11: Protected Fixed Media Device backup rule type

A new Protected Fixed Media Device (PFMD) backup rule type stores backup data on the protected partition (/p) of the CS 1000 system. CP PII systems store the backup data on a local hard drive. CP PIV systems use an onboard CF card.

The number of backup versions is defined during rule creation; however, the default value is 1. Each backup file is numbered. The most current version is stored in bkdata.1 By default, this rule is predefined on the system and scheduled to perform a backup to the /p/bkbp/backup directory every 7 days (Saturday at 3AM local time).

You can modify or remove the rule or schedule using the existing backup rule and schedule configuration options in Element Manager or LD 117.

For more information about configuring PFMD backup rules, see *System Redundancy Fundamentals, NN43001-507*.

Chapter 12: Shared Bandwidth Management

The Shared Bandwidth Management (SBWM) feature allows sharing of bandwidth between multiple servers and/or bandwidth consumers in a single location. Bandwidth is dynamically allocated between video and voice by Avaya Aura Session Manager (SM), which shares the bandwidth management responsibilities with all SIP entities using a common interface, PUBLISH API.

The Avaya Aura SM manages bandwidth using the concept of locations. The location concept is analogous to bandwidth zones on the Call Server. In order to comply with the Avaya Aura SM location scheme, the Call Server uses zone names. A zone name corresponds to a location on the Session Manager.

For additional details about SBWM, see *Converging the Data Network with VoIP Fundamentals, NN43001-260*.

SBWM requires the following Call Server configuration:

- Zone names must correspond to Avaya Aura SM location names.
- Enable SBWM on outgoing SIP routes.
- Determine the Reserved Bandwidth Block Size.

For more information about Call Server configuration, see *Converging the Data Network with VoIP Fundamentals, NN43001-260*.

SBWM requires the following Avaya Aura SM configuration:

- Configure a SIP entity with the Call Admission Control option.
- Configure the SIP entity as a shared bandwidth manage.

For more information about Avaya Aura SM configuration, see *Administering Avaya Aura ® Session Manager.*

Chapter 13: Unregistered Phone Notification

UPND/UPNA is introduced as a new option in Element Manager and LD 15 in Release 7.6. This feature allows the user to enable the Unregistered Phone Notification capability. Currently when a call is directed to an IP phone that is not registered, the caller hears a ringback tone. The new Unregistered Phone Notification option, when enabled, provides a Destination Unregistered notification to the caller of the IP phone that isn't registered.

If the called set is not registered and has not been configured with Call Forward No Answer feature, the call will be released and the caller will hear the fast busy reorder tone. The caller's display indicates that the **Destination is unregistered**. This feature is included in base system software.

For more information, see "**Unregistered Phone Notification**" in *Features and Services Fundamentals-Book 6, NN43001-106-B6.*

Chapter 14: Upgrade and New Install applications

The Upgrade and New Install applications are components of the Health Check Tool introduced in Release 7.6 to provide guidance through the major steps of the upgrade and new installation processes. The upgrade application does not change the installation programs of the various system elements. It simply guides the user through each process by identifying the required tasks and recommending best practices, such as capturing critical pre-upgrade information. The actual installation/upgrade tasks are performed manually under the direction of the appropriate application. The application provides the user with an estimated completion time for each task and references to proper documentation and/or a best practices checklists.

For more information on the Upgrade and New Install applications, see *NN43001–408, Upgrades Guide*.

Chapter 15: Voice mail soft keys enable/ disable for CallPilot

A new Class of Service VMSA/VMSD is introduced in Element Manager and LD 11 to enable Voice Mail (VM) context-sensitive soft keys on IP Deskphones with UNIStim software and on 3900 series Digital Telephones. The VM soft keys are displayed when the user presses the Messages/Inbox key (internal and external) or manually dials their voice mail access number (internal only). The VM context-sensitive soft keys feature is enabled by default.

The displayed soft keys are CallPilot-specific, and may not apply to third-party voice mail systems. Avaya recommends that the VM soft key feature be disabled on systems not using CallPilot.

There are no minimum UNIStim or CallPilot software requirements.

For more information, see "**Voice mail soft keys enable and disable**" in *Features and Services Fundamentals-Book 6, NN43001-106-B6.*

Chapter 16: Software Input/Output prompts, responses and commands

The information in this chapter outlines the new, changed, or retired information in the*Software Input/Output Reference-Administration document (NN43001-611)* and *Software Input/Output Reference-Maintenance document (NN43001-711)* for Avaya Communication Server 1000 Release 7.6.

New in this release

The following tables detail what's new in this document for Avaya Communication Server 1000 Release 7.6.

Table 1: Prompts and Responses

Prompt	Response	Comment
CDR Call Disconnect by Trunk/Line side		
LD 15 Call Detail Recording		
ACDD	(NO) YES	Allow or deny ACD Detailed option
Mobile Extensions		
LD 16 Route Data Block		
MBRA	(YES) NO	Mobile Route Access (package 412 MOBX must be equipped).
LD 21 Print Routine 2		
Route Data Block		
MBRA	<yes>,<no>	Mobile Route Access
Shared Bandwidth Management		
LD 16 Route Data Block		
SBWM	(NO) YES	Allow or deny Shared Bandwidth Management
Flexible Calling Line ID		
LD 86 FEAT equal to CMDB Data Block		
MID	X....X	Matching initial digits — up to 16 digits.

Prompt	Response	Comment
INST	X....X	Insert initial digits — up to 16 digits.

Table 2: Alphabetical List of Prompts

Prompt	Response	Comment	Pack/Rel
Voice Mail Context-sensitive Soft Keys			
LD 11 Class of Service			
CLS	(VMSD)	Voice Mail Soft keys denied.	basic-7.60
	VSMA	Voice Mail Soft keys allowed.	
Unregistered Phone Notification			
LD 15 Features and options			
OPT	(UPND)	Unregistered Phone Notification Denied	basic-7.60
	UPNA	Unregistered Phone Notification Allowed	
Mobile Extensions			
LD 16 Route Data Block			
MBRA	(YES) NO	Mobile Route Access for Mobile Extension. Where: • YES = Any incoming calls are allowed via this route to a local set. • NO = Only mobile set can make calls to local set via this route. Prompted when MBXR = YES. Package 412 MOBX must be equipped.	mobx-7.60
LD 21 Print Routine 2			
Route Data Block			
MBRA	<yes>,<no>	Mobile Route Access	mobx-7.60
Shared Bandwidth Management			
LD 16 Route Data Block			
SBWM	(NO) YES	Allow or deny Shared Bandwidth Management	basic-7.60
Flexible Calling Line ID			
LD 86 FEAT equal to CMDB Data Block			
MID	x...x	Matching Initial Digits, up to 16.	basic-7.60
MNUM	a...a	Matching Number Type. Where a...a is: • (DC) = Don't Change • CLNG = Calling Number	basic-7.60

Prompt	Response	Comment	Pack/Rel
		• CONN = Connected Number • OCN = Originally Called Number	
MTON		Matching Type of Number (a...a = UKWN, INTL, NATL, SPN, LOCL, ELOC, CDP, CSS7, NCHG)	basic-7.00
		Note: With release 7.6, NCHG is replaced with DC (Don't Change)	basic-7.60
RNPI	a...a	Replacement Numbering Plan Indicator (a...a = E164, PRIV, E163, TELE, X121, NATL, NCHG)	basic-7.00
		Note: With release 7.6, NCHG is replaced with DC (Don't Change)	basic-7.60

Table 3: Alphabetical List of Commands

Command	Description	Pack/Rel
LD 117 Change backup rule to Protected Fixed Media Device (PFMD)		
Alphabetical list of Administration commands		
`CHG BKPR <rule number 1-100> PFMD [<N of versions>] [<name>]`	Change backup rule to Protected Fixed Media Device (PFMD), where: • rule number = 1-100. You can define up to 100 backup rules. Once defined, a rule can also be applied as a template for creating new backup rules. PFMD rules can be used by automatic backup schedules or by manual backup and restore operations (BKR/RSR commands activated from LD 43). • PFMD = mnemonic for this rule type. • N of versions = (1)-10 number of incremental backup data versions preserved on the local hard disk. • name = rule name, of up to a maximum of 30 text characters (without white spaces).	basic-7.60
LD 117 Shared Bandwidth Management		
Alphabetical list of Administration commands		
`CHG SBWM <zone number> [<ReserveBandwidthBlockSize>]`	Change the Bandwidth Reservation Block Size	basic-7.60

Command	Description	Pack/Rel
	Note: Bandwidth Block Size is an optional parameter and when omitted the previous Bandwidth Block Size value is used.	
`CHG ZNAME <zone number> <zone name>`	Configure a Zone Name for a bandwidth zone **Note:** Zone Name is case sensitive.	basic-7.60
Alphabetical list of Maintenance commands		
`DIS SBWM ALL`	Disables SBWM for all zones.	basic-7.60
`ENL SBWM ALL`	Enables SBWM for all zones configured with non-zero location names.	basic-7.60
`ENL SBWM <zone number> <BW Block Size>`	Enables SBWM for a particular zone and establishes Reserved Bandwidth Block Size.	basic-7.60
`OUT ZNAME <zone number>`	Remove zone location name for zone number.	basic-7.60
`PRT SBWM <zone number/ALL>`	Prints Shared Bandwidth Management information: Zone Number; Zone Name; SBWM status; and configured Reserved Bandwidth Block Size (kbps).	basic-7.60
`PRT ZNAME <zone number/ALL>`	Prints the Zone Number and Zone Location Name.	basic-7.60
`STAT SBWM <zone number/ALL>`	Displays zone statistics and the status of SBWM and Reserved Bandwidth Block Size. SBWM statistics displayed are: • Zone Number • SBWM Status • Used Bandwidth • Total Calls • BW Usage % • BW Pool Size • BW Peak Pool	basic-7.60

Command	Description	Pack/Rel
	• BW Block Size • BW Incremtenal Request • BW Decremtenal Request • Blocked Calls • Request While Pending • Maximun Offline BW	
`RESET SBWM STATS <zone number>`	Reset some SBWM statistics displayed by STAT SBWM. **Note:** Since the stats are cumulative from the last reboot it may be desirable to reset them to monitor for a particular time period. When the zone number is not specified all the zones will be reset. Status report fields reset are: • Total Calls • BW Peak Pool • BW Incremtenal Request • BW Decremtenal Request • Blocked Calls • Request While Pending	basic-7.60

New in this release

The following tables detail what's new in this document for Avaya Communication Server 1000 Release 7.6.

Table 4: Commands

Command	Description	Pack/Rel
LD 32 DSP Status Report command		
ECNT DSP mm	Prints a summary message containing status for DSP resources every **mm** minutes. Where **mm** equals the report period: **0** (disabled), 15, 30, or 60 minutes. The output includes the following:	basic-7.60

Command	Description	Pack/Rel
	INFO0002 LD32 ECNT DSP IDLE:xx BUSY:yy OOS:zz hh:mm:ss dd/mm/yyyy	
LD 96 D-channel Call Trace (DCT) tool		
`DCT dch [<d1>..<d10>] ras [on|off] cr <mode>`		basic-7.60
	Specify specific types of RAS and CR options for monitoring. Where: • dch = option of the DCT which changes D-channel settings • <d1>..<d10> = D-channel numbers, can be configured to a maximum of ten numbers • ras = Return Address Stack (RAS) option. Where: - on = enables the RAS option - off = disables the RAS option for the specified <d1>..<d10> D-channels. By default, the RAS option is disabled. • cr = Call Register (CR) option. The value is <mode>. The CR mode can be a value from 0 to 3, where: - 0 – does not collect Call Register data. Default value. - 1 – collect CRPTR data only - 2 – collect MSGCR data only - 3 – collect both CRPTR and MSGCR data Examples: dct dch 0 2 ras on cr 3 – enables RAS option and set CR mode 3 for D-channels 0 and 2. Configure these D-channels to be monitored by the DCT tool. dct dch 3 ras off cr 2 – disable RAS option and set CR mode 2 for D-channel 3. Configure this D-channel to be monitored by the DCT tool. dct dch 1 ras off cr 0 or dct dch 1 – both RAS and CR options are disabled. Configure D-channel 1 to be monitored by the DCT tool.	
DCT I [<xxxxxxxx> | all] <NPI> <TON> <msgRecv> <msgSend> [<c1> <c2> <c3>]		basic-7.60
	Specify specific types of calls, specified message type and cause value for monitoring. Where: • i = index number from 1 to 5 • xxx|all = the dialing/dialed number to be monitored - <xxx> = DN or part of the DN; it can be from 2 to 8 digits - all = monitors all DN numbers	

Command	Description	Pack/Rel
	• NPI = Numbering Plan Index; value from 0 to 7: - 0 – filtering off; used by default - 1 – UNKNOWN - 2 – PRIVATE - 3 – ISDN (E.164) - 4 – E.163 - 5 – TELEX - 6 – DATA - 7 – NATIONAL • TON = Type of Number; value from 0 to 7 - 0 – filtering off, used by default - 1 – UNKNOWN - 2 – INTERNATIONAL - 3 –NATIONAL - 4 - NETWORK SPECIFIC - 5 – SUBSCRIBER - 6 – LEVEL 1 REGIONAL - 7 – LEVEL 0 REGIONAL • msgRcv = incoming message type, value from 0 to 255 or off - • off – filtering off; used by default - • 0 – 255 – a value in decimal format equal to the required message type in the source (value of the required message type constant). For example: **SETUP** message type for PRA trunks type has the constant **.PRA_SETUP** and its value is **4**. UIPE trunks has the constant **.CC_SETUP_REQ** and its value is **14**. • msgSnd = outgoing message type, value from 0 to 255 or off - • off – filtering off; default value - • 0 – 255 – a value in decimal format equal to the required message type in the source (value of the required message type constant). For example: The **DISCONNECT** message type for PRA trunks type has the constant **.PRA_DISCONN** and its value is **7**.	

Command	Description	Pack/Rel
	UIPE trunks has the constant **.CC_DISC_REQ** and its value is **2**. • <c1> <c2> <c3> = cause value; value from 0 to 127. Zero is the default value. Up to three different reasons, separated by a space, can be configured. - 0 – filtering off; default value - 1 – 127 – value of the cause in decimal format equal to the required reason in the source (value of the required cause constant). For example: The reason Normal Call Clearing has the constant **.PRA_NORM_CLR** and its value is **16**. The reason User Busy has the constant **.PRA_USER_BUSY** and its value is **17**.	
LD 117 Change backup rule to Protected Fixed Media Device (PFMD) **Alphabetical list of Administration commands**		
`CHG BKPR <rule number 1-100> PFMD [<N of versions>] [<name>]`	Change backup rule to Protected Fixed Media Device (PFMD), where: • rule number = 1-100. You can define up to 100 backup rules. Once defined, a rule can also be applied as a template for creating new backup rules. PFMD rules can be used by automatic backup schedules or by manual backup and restore operations (BKR/RSR commands activated from LD 43). • PFMD = mnemonic for this rule type. • N of versions = (1)-10 number of incremental backup data versions preserved on the local hard disk. • name = rule name, of up to a maximum of 30 text characters (without white spaces).	basic-7.60
LD 117 Shared Bandwidth Management **Alphabetical list of Administration commands**		
`CHG SBWM <zone number> [<ReserveBandwidthBlockSize>]`	Change the Bandwidth Reservation Block Size **Note:** Bandwidth Block Size is an optional parameter and when omitted the previous Bandwidth Block Size value is used.	basic-7.60
`CHG ZNAME <zone number> <zone name>`	Configure a Zone Name for a bandwidth zone	basic-7.60

Command	Description	Pack/Rel
	Note: Zone Name is case sensitive.	
Alphabetical list of Maintenance commands		
`DIS SBWM ALL`	Disables SBWM for all zones.	basic-7.60
`ENL SBWM ALL`	Enables SBWM for all zones configured with non-zero location names.	basic-7.60
`ENL SBWM <zone number> <BW Block Size>`	Enables SBWM for a particular zone and establishes Reserved Bandwidth Block Size.	basic-7.60
`OUT ZNAME <zone number>`	Remove zone location name for zone number.	basic-7.60
`PRT SBWM <zone number/ALL>`	Prints Shared Bandwidth Management information: Zone Number; Zone Name; SBWM status; and configured Reserved Bandwidth Block Size (kbps).	basic-7.60
`PRT ZNAME <zone number/ALL>`	Prints the Zone Number and Zone Location Name.	basic-7.60
`STAT SBWM <zone number/ALL>`	Displays zone statistics and the status of SBWM and Reserved Bandwidth Block Size. SBWM statistics displayed are: • Zone Number • SBWM Status • Used Bandwidth • Total Calls • BW Usage % • BW Pool Size • BW Peak Pool • BW Block Size • BW Incremtenal Request • BW Decremtenal Request • Blocked Calls • Request While Pending	basic-7.60

Command	Description	Pack/Rel
	• Maximun Offline BW	
`RESET SBWM STATS <zone number>`		basic-7.60
	Reset some SBWM statistics displayed by STAT SBWM. **Note:** Since the stats are cumulative from the last reboot it may be desirable to reset them to monitor for a particular time period. When the zone number is not specified all the zones will be reset. Status report fields reset are: • Total Calls • BW Peak Pool • BW Incremtenal Request • BW Decremtenal Request • Blocked Calls • Request While Pending	

Chapter 17: System messages

The following Chapter describes the system messages that are introduced for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.6.

The following information is available for each system message:

- message description
- action (if applicable)
- message severity
- whether the message is critical to monitor
- whether the message is sent as an SNMP trap

AUD: Software Audit (LD 44)

The following table contains the AUD system messages introduced in Release 7.6.

Table 5: AUD messages

Message	Description	Action	Severity	Monitor	SNMP
AUD0131	Call Wait Tone CR is lost. The main CR is idle but the Call Wait Tone CR remains. The CR information: CR, AUXPM, MAINPM, ORIGTYPE, ORIGTN, TERTYPE, TERTN, QUEUE IN.		Minor	False	True
AUD0132	TN of stuck SIPL set, TIME, Reason (Integer number) SIPL IP Phone is stuck in the current state	Contact your next-level technical support.	Info	False	False
AUD0133	Special call register MAINPM = .SPECIAL, AUXPM		Warning	False	False

Message	Description	Action	Severity	Monitor	SNMP
	= .IAGT_ADCR_MA is in an invalid state or queue.				

BUG: Software Error Monitor

The following table contains the BUG system messages introduced in Release 7.6.

Table 6: BUG messages

Message	Description	Action	Severity	Monitor	SNMP
BUG0794	Local IPsec status and remote IPsec status do not match, local (lstate), remote (rstate) Where: (lstate) = Enabled or Disabled (rstate) = Enabled or Disabled A mismatch between the local IPsec status and remote IPsec status allows you to establish a secure link with only one CPU core in a High Availablility system.	Check that active and inactive CS have IPsec configured both as (yes) or both as (no) in UCM. If the problem persists, contact your next-level technical support.	Critical	True	True
BUG0795	Invalid tds slot procedure WRITE_SERV_CIRC A request to provide a tone has failed.	If the problem persists, contact your next-level technical support.	Info	False	False
BUG0796	Corrupted High or Low priority Input Buffer. An automatic system WARM star occurs to rebuild the input buffers.	Provide the rpt report to your next-level technical support.	Major	True	True

DTA: Digital Trunk Diagnostic

The following table contains the DTA system messages introduced in Release 7.6.

Table 7: DTA messages

Message	Description	Action	Severity	Monitor	SNMP
DTA0031	Loop alarm states status response. (text) The values of IMSG_G_LOOP, PRI2_I_LOS and PRI2_I_AIS are printed.		Info	False	False
DTA0032	Loop alarm states status response (Continued) (text) The values of PRI2_I_LFAS, PRI2_LMAS and PRI2_I_RAI are printed.		Info	False	False

ERR: Error Monitor (Hardware)

The following table contains the ERR system messages introduced in Release 7.6.

Table 8: ERR messages

Message	Description	Action	Severity	Monitor	SNMP
ERR0037	ERR0037 (Reason Code) (TN) Where Reason code is, 1. H.323 Virtual Trunks exceeded Limit. 2. SIP Virtual Trunks exceeded Limit. 3. Total Virtual Trunks Exceeded Limit. TN : The Channel for which the registration failed. 4. Configure a single SS node with SIP VTRK. 5. Note the error messages on the Call Server when the 1801's trunk attempts to register.		Minor	False	False

Message	Description	Action	Severity	Monitor	SNMP
	6. SIPL VTRK exceeds the maximum. 7. SIPL is not enabled by the application. 8. There is a version mismatch between the Call Server and the Signaling Server.				

INFO: Informational messages

The following table contains the INFO system messages introduced in Release 7.6.

Table 9: INFO messages

Message	Description	Action	Severity	Monitor	SNMP
INFO0002	LD32 ENCT DSP IDLE:xxx BUSY:yyy OOS:zzz hh:mm:ss dd/mm/yyyy System DSP Status output from LD32 ECNT DSP command		Info	False	False

MEM: Memory Management

The following table contains the MEM system messages introduced in Release 7.6.

Table 10: MEM messages

Message	Description	Action	Severity	Monitor	SNMP
MEM0122	TrMem mem block error The tr mem library encountered an internal error. The error should not impact the system, but it could indicate a serious software problem.	If the problem persists, contact your next-level technical support.	Major	True	True

Message	Description	Action	Severity	Monitor	SNMP
MEM0123	TrMem Malloc failed The system is out of memory.	You must reboot the system. If the problem persists, contact your next-level technical support.	Critical	True	True
MEM0124	TrMem lib invalid pointer An invalid pointer has been detected. The error should not impact the system, but it could indicate a serious software problem.	If the problem persists, contact your next-level technical support.	Major	True	True
MEM0125	TrMem Block header corruption There is an overflow in a memory buffer. The error should not impact the system, but it could indicate a serious software problem.	If the problem persists, contact your next-level technical support.	Major	True	True
MEM0126	TrMem did not create memory pool \ The system is out of memory.	You must reboot the system. If the problem persists, contact your next-level technical support.	Critical	True	True
MEM0127	SeaWeed Mem library memory buffer overflow There is an overflow in a memory buffer. The error should not impact the system, but it could indicate a serious software problem.	If the problem persists, contact your next-level technical support.	Major	True	True

PCH: System Patch Reports

The following table contains the PCH system messages introduced in Release 7.6.

Table 11: PCH messages

Message	Description	Action	Severity	Monitor	SNMP
PCH0226	Removes the obsolete patch with handle %d.		Info	False	True

Message	Description	Action	Severity	Monitor	SNMP
PCH0227	Patch %d has special instruction at the time of loading.		Info	False	True
PCH0228	Patch %d has special instruction at the time of deactivating.		Info	False	True
PCH0229	Dependent patch %s must be activated first. A dependant patch must be enabled before the current patch installation can be completed.	You must activate the dependant patch first.	Warning	False	True
PCH0230	Dependent patch %s must be removed first. The dependant patch must be removed before current patch can be inserted.	Remove the dependant patch.	Warning	False	True
PCH0231	Cannot allocate memory for dependent patch name of patch %s. The system could not allocate memory for dependant patch	Contact your next-level technical support.	Critical	True	True
PCH0232	Cannot allocate memory for number of obsolete patches for patch %s. The system could not allocate memory for patch list.	Contact your next-level technical support.	Critical	True	True
PCH0233	Cannot allocate memory for patch obsolete patches names for patch %s. The system could not allocate memory for obsolete patch list.	Contact your next-level technical support.	Critical	True	True
PCH0235	Error in reading %s patch footer information. The patch file may be corrupted and cannot be installed	Contact your next-level technical support.	Major	True	True
PCH0236	Error in opening patch file %s. The patch file may be corrupted and cannot be installed.	Contact your next-level technical support.	Major	True	True

Message	Description	Action	Severity	Monitor	SNMP
PCH0237	Plugin x has been enabled.		Info	False	False
PCH0238	Plugin x has been disabled.		Info	False	False
PCH0239	Plugin x has been disabled because it is suspected to cause inits.		Info	False	False

SCH: Service Change

The following table contains the SCH system messages introduced in Release 7.6.

Table 12: SCH messages

Message	Description	Action	Severity	Monitor	SNMP
SCH0223	Member number out-of-range (1-254).		Info	False	False
SCH0593	Member number incremented past limit (254). No more trunks can be added.		Info	False	False
SCH1398	Zone configuration is incorrect: x Where x is one of the following configuration errors: • SBWM is not supported for VTRK zone • Zname must be 63 chars • Zname already exists • RESERVED BLOCKSIZE must be at least 200kbps • Zone does not exist • Zone already configured • Zone is used		Info	False	False

Message	Description	Action	Severity	Monitor	SNMP
	• Entered bandwidth value is less than currently used • Invalid daylight saving time values				
SCH1572	Invalid Repeat Counter for this type of trunk, Max=254.Only WATTS, FEX, DID, COT, TIE, ISA, CBCT, FGDT, IRAN and IMUS trunk types have a higher limit.		Info	False	False
SCH1573	Member number incremented past limit (510). No more trunks can be added.		Info	False	False
SCH1574	Member number incremented past limit (3700). No more trunks can be added.		Minor	False	False
SCH2308	You cannot change IPMG type unless you delete all VGW channels for the IPMG first. Changing the IPMG type is restricted because the current configuration of VGW channels may not be supported by another IPMG type.	Delete all configured VGW channels for the IPMG before changing the IPMG type.	Info	False	False
SCH2425	ISM limit of IP Music connections (IP MUS CON) is equal to 0. You cannot decrement the ISM limit because it equals 0.		Warning	False	False
SCH2426	Repeat count out of range (2-4000). Further limits are based on TYPE.		Info	False	False
SCH2427	You must set the PSDN while in PREA mode. If you do not specify the PSDN it can result in a	Specify the PSDN if it is undefined.	Info	False	False

Message	Description	Action	Severity	Monitor	SNMP
	failure to send Presence messages.				
SCH2428	You are not permitted to change the existing IPMG loop type to/from MGX.	Configure a new IPMG loop with the required type.	Info	False	False
SCH2429	You cannot create a PFMD rule by default; there are no available rule and schedule items. PFMD rule is not created automatically.		Minor	False	False
SCH2430	Cannot change the UXTY from or to IMSL.	Use OUT and NEW to change the type of UXTY for this unit.	Info	False	False

SRPT: System Reports

The following table contains the SRPT system messages introduced in Release 7.6.

Table 13: SRPT messages

Message	Description	Action	Severity	Monitor	SNMP
SRPT0337	Failed to initialize the FMD; remove the RMD immediately. The FMD can become inaccessible if problems occur with the inserted RMD.	Immediately remove the RMD. Further use of the problem RMD is not recommended.	Critical	True	True
SRPT0338	Too many force sync retries attempted (queue high water mark) This may indicate that the LD 135 system state is stuck in SYNCING state.	Check the system state in LD 135. If it is in SYNCING state for an extended period of time then perform an INI of the inactive core; otherwise no action is required. If the problem persists, contact your next-level technical support.	Minor	False	False
SRPT0339	Incremental backup to local PFMD failed.		Minor	False	False

Message	Description	Action	Severity	Monitor	SNMP
	Backup of data files to the protected partition /p failed.				
SRPT0340	The PFMD backup rule is set by default. The PFMD rule is created automatically and uses the default schedule. All backup data files are stored each Monday at 3:00 AM on the proteted /p partition.		Minor	False	False
SRPT0341	The system cannot create a PFMD rule by default; there are no available rule and schedule items. PFMD rule is not created automatically.		Minor	False	False
SRPT0342	Warning: source is truncated. Part of the information you have entered has been truncated and is not added to /e/trace/ OVLChange.ovl log file. The information you enter cannot exceed the MAX buffer size (20,000 chars).		Warning	False	True
SRPT0343	Connection with IPMG (IPMG number) (card number) is UP.		Cleared	False	True
SRPT0344	The socket file descriptors in an unbound state are closed.		Info	False	False

SYS: System Loader

The following table contains the SYS system messages introduced in Release 7.6.

Table 14: SYS messages

Message	Description	Action	Severity	Monitor	SNMP
SYS0188	Multiple PFMD backup rules defined. Multiple PFMD backup rules are not permitted. All PFMD rules will be removed except the first one.		Minor	False	False
SYS0189	Failed to create default PFMD backup rule or schedule, cannot allocate protected memory. PFMD rule is not created automatically. For functionality to work, it must be created manually.		Minor	False	False
SYS0192	Data for unsupported feature is cleared or de-allocated.		Info	False	False
SYS0193	Trunk TN loaded but route data block is not found. TN is deleted. This message is printed once for each contiguous grouping of TNs in the same customer and route.	Check and rebuild route and trunk data as required. If a previous message reported a trunk route being deleted this message is expected.	Info	False	False

TFS: Traffic Measurement

The following table contains the TFS system messages introduced in Release 7.6.

Table 15: TFS messages

Message	Description	Action	Severity	Monitor	SNMP
TFS0304	Traffic counts may have incorrect values because the current system time was changed by Network Time Protocol.		Warning	False	False

Index

A

R

V