New in this Release
Avaya Communication Server 1000

7.5
NN43001-115, 05.07
August 2011

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 generally makes available to users of its products. 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 Web sites 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 its Hardware and Software (“Product(s)”). 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. 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 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

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.

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

Revision history

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

Avaya Communication Server (Avaya CS 1000) Release 7.5 is the latest release for the Avaya CS 1000 family of products. CS 1000 Release 7.5 is a further evolution of the traditional TDM enterprise network to a converged IP based network.

The CS 1000 Release 7.5 is a reliable and secure platform for Voice over IP (VoIP) communications and is designed to be a more open and simplified platform, which speeds deployment and improves manageability.

Key Attributes

- Adaptable to meet current and future needs

  Delivers investment protection and evolution path to next-generation multimedia communications

- Superior IP Telephony experience

  More open platform to take advantage of innovative applications, and feature-rich next generation clients

- Improved reliability and security

  Business continuity improvement from a reliable and secure environment

- Simplified convergence solution

  Product portfolio simplified for easier deployment, configuration and management

New for CS 1000 Release 7.5

The following sections provide a description of what's new in Avaya Communications Server 1000 (CS 1000) Release 7.5.

CS 1000 Release 7.5 offers complete Avaya Aura® Integration. Avaya Aura® extends the capabilities of migrated CS 1000 systems, which subsequently provide faster and easier deployment of voice, video, messaging, and presence services.

For CS 1000 Release 7.5, Avaya Aura® System Manager 6.1 is required for managing systems with Avaya Aura® Session Manager or Avaya Aura® Presence Services. The functionality of UCM and Subscriber Manager is now available in System Manager. All existing systems with

a Network Routing Service (NRS) must migrate to Session Manager, with the following exceptions:

- Migration support for customers with multiple NRS
- H.323 Gatekeeper
- IPv6 support
- Communication Sever 1000E High Scalability
- Survivable SIP MG Tertiary NRS server

In networks that do not use Avaya Aura® Session Manager or Avaya Aura® Presence Services, you can continue to use UCM without migrating to System Manager for CS 1000 Release 7.5.

Note:

- 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 is available, the term Subscriber Manager in the documentation refers to Subscriber Manager in System Manager; on systems where System Management 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.

Note:

Media encryption is disabled for CS 1000 systems sold in Russia, Belarus, and Kazakhastan. For more information, see the CS 1000 Product Bulletin.

Packages

There are no new packages introduced for this release.

Hardware

Communication Server 1000 Release 7.5 introduces a new commercial off-the-shelf (COTS) server.

HP DL360 G7 server

This server provides the next iteration of the COTS platform providing enhanced processing power. For more information about the HP DL360 G7 server, see Commercial off-the-shelf servers on page 39.

Documents

The following documents are retired for Avaya CS 1000 Release 7.5:

- *Secure Multimedia Controller 1.0 Command Reference , NN43001-119*
- *Secure Multimedia Controller 1.1 Fundamentals (NN43001-325)*
- *Attendant PC Console Fundamentals (NN43001–520)*

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 12 shows an example and how to interpret the task flows.

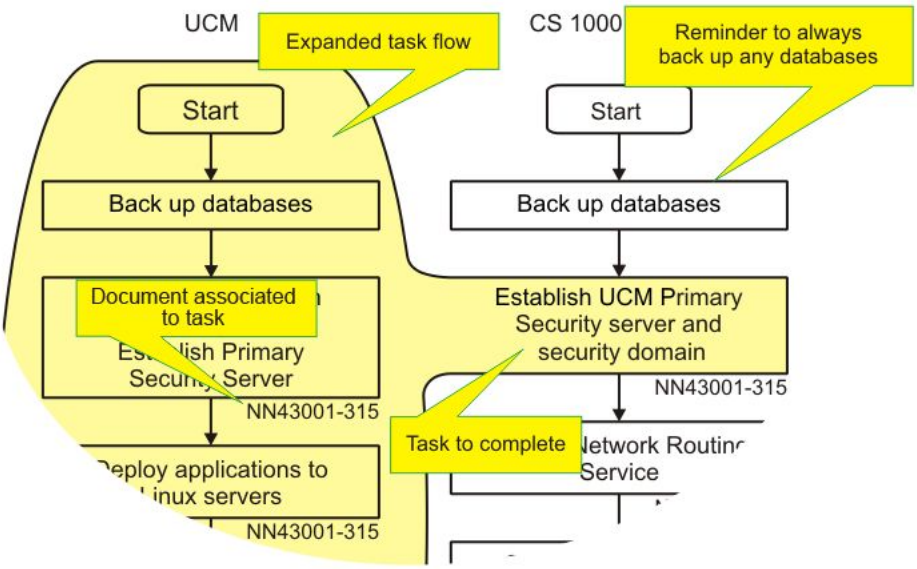

Figure 1: Example task flow

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)*
- *SIP Trunk Bridge Fundamentals , NN43001-143*

- *IP Peer Networking Installation and Commissioning , NN43001-313*
- *Communication Server 1000E High Scalability Installation and Commissioning, NN43041-312*

Network

Figure 2: Network task flow on page 14 appears in *Planning the Network-wide Upgrade, NN43001-406*.

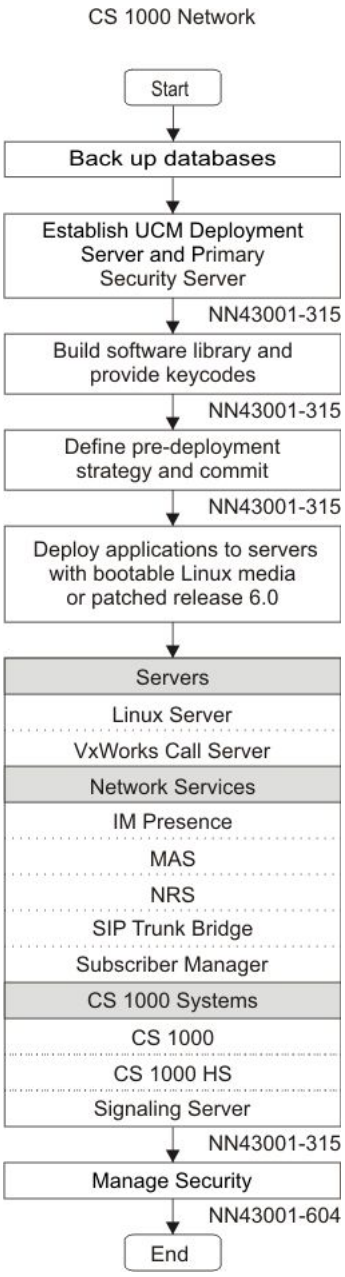

Figure 2: Network task flow

Linux base and UCM

Figure 3: Linux base and UCM task flow on page 15 appears in *Linux Platform Base and Applications Installation and Commissioning, NN43001-315* and *Unified Communications Management Fundamentals , NN3001-116*.

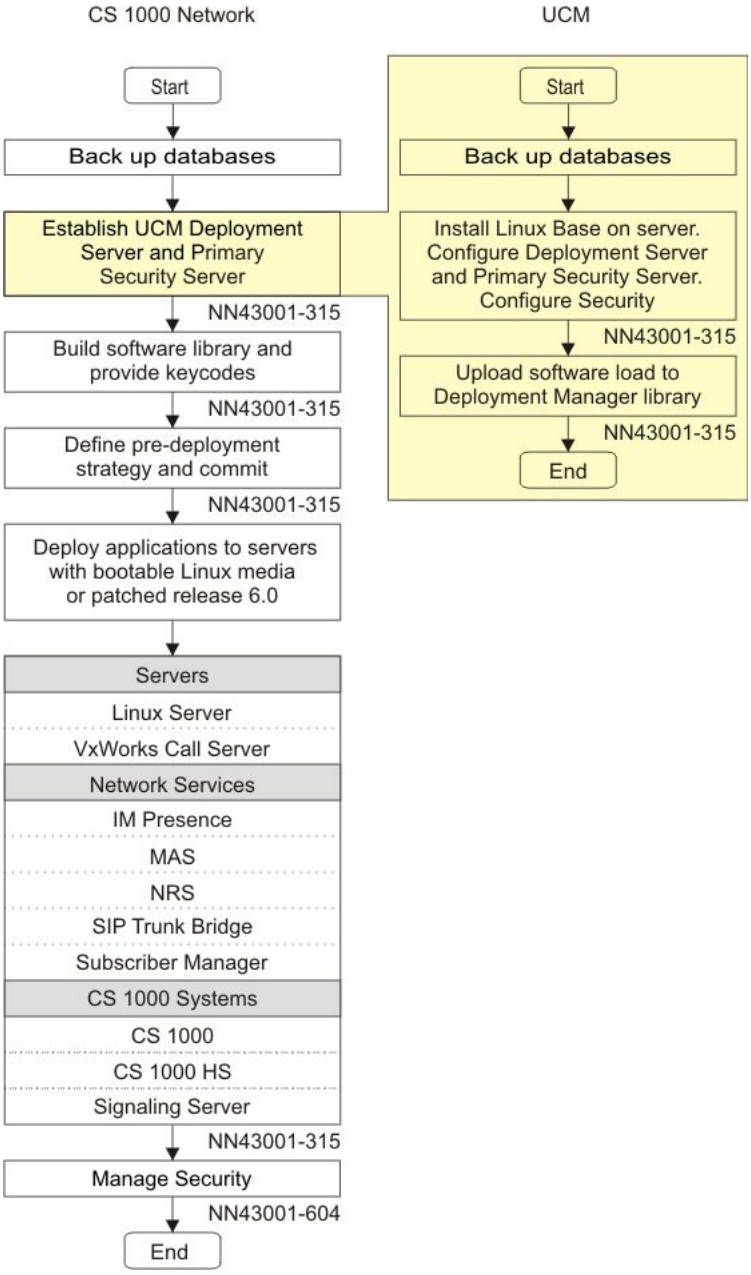

Figure 3: Linux base and UCM task flow

Migration from CS 1000 to Avaya Aura

Figure 4: Migration task flow on page 16, Figure 5: Migration task flow cont on page 17, Figure 6: Migration task flow cont on page 18, andFigure 7: Migration task flow cont on page 19 appear in *Planning the Network-wide Upgrade, NN43001-406*.

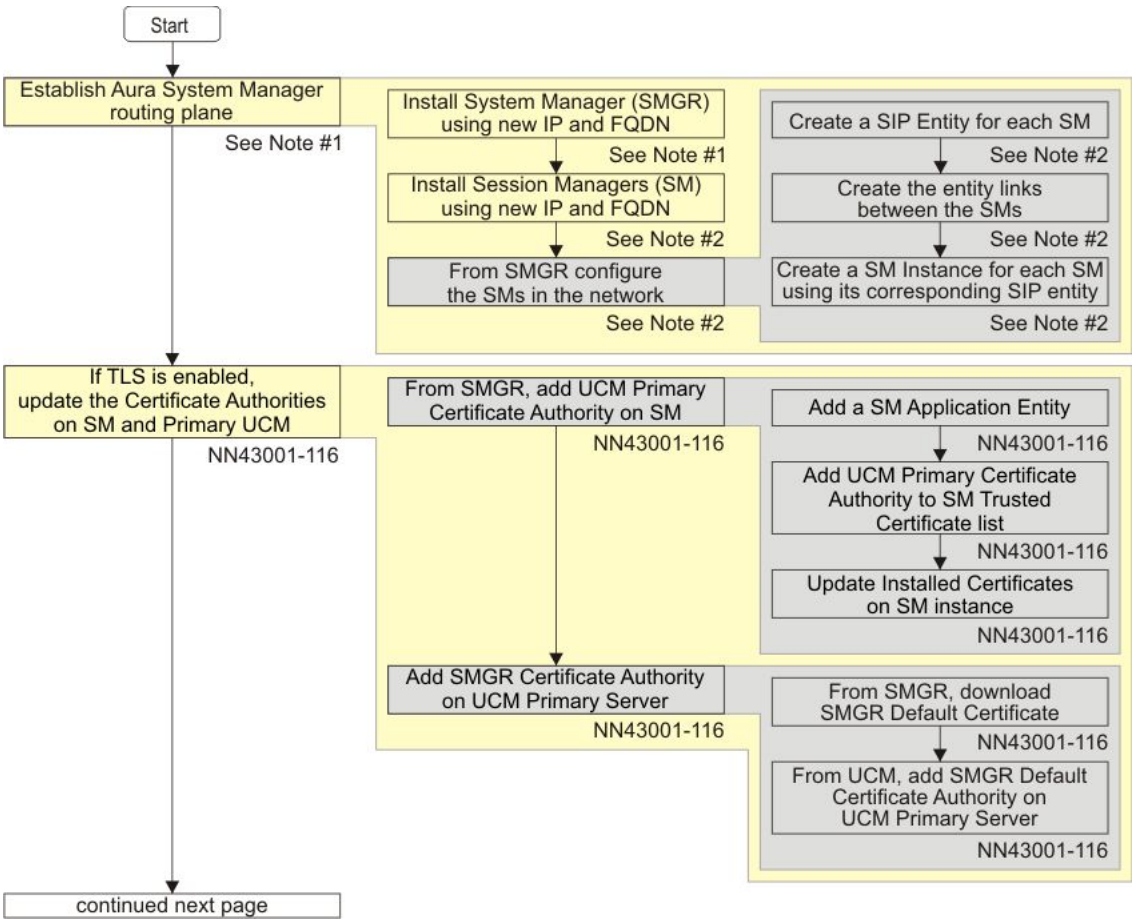

Figure 4: Migration task flow

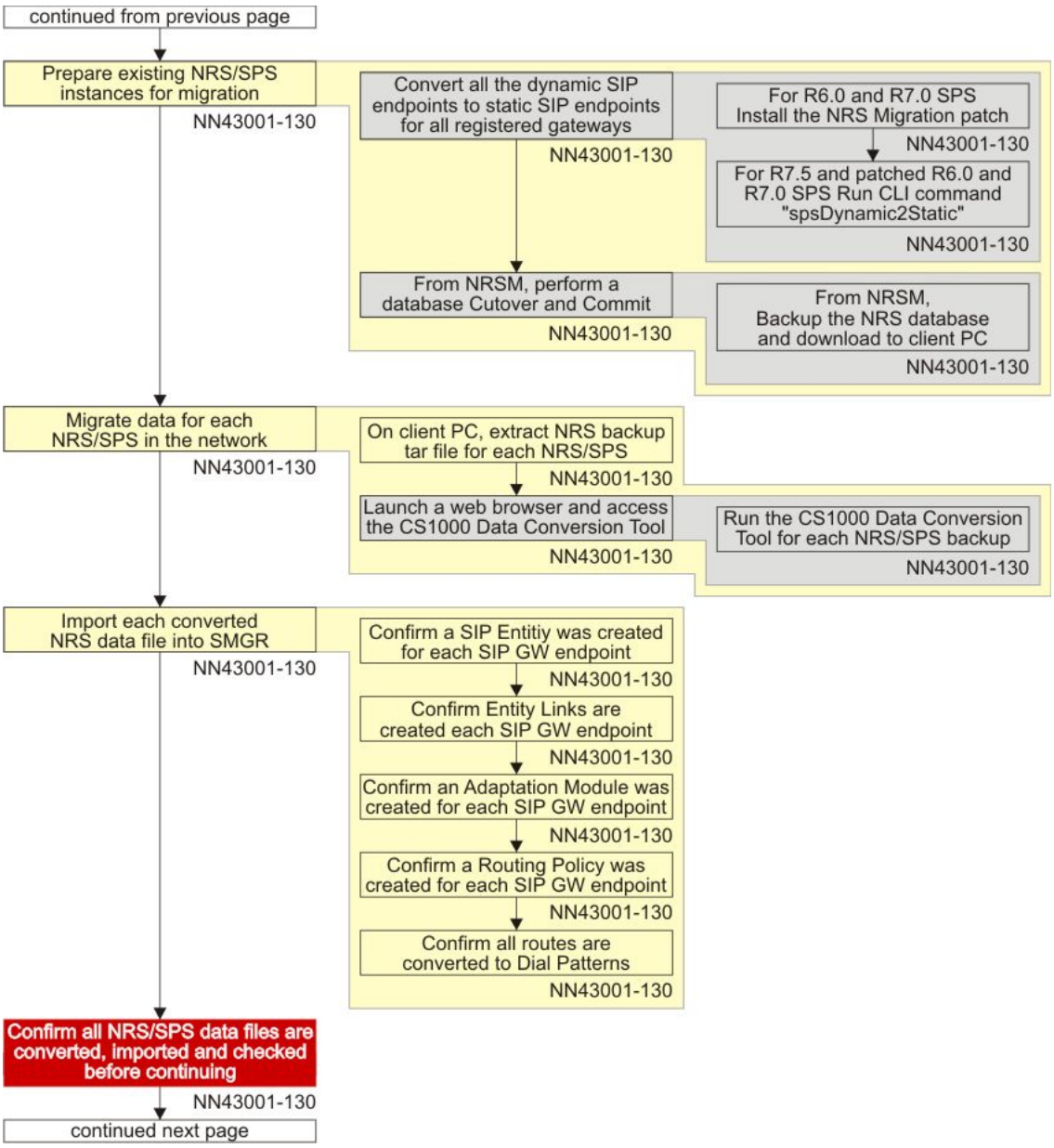

Figure 5: Migration task flow cont

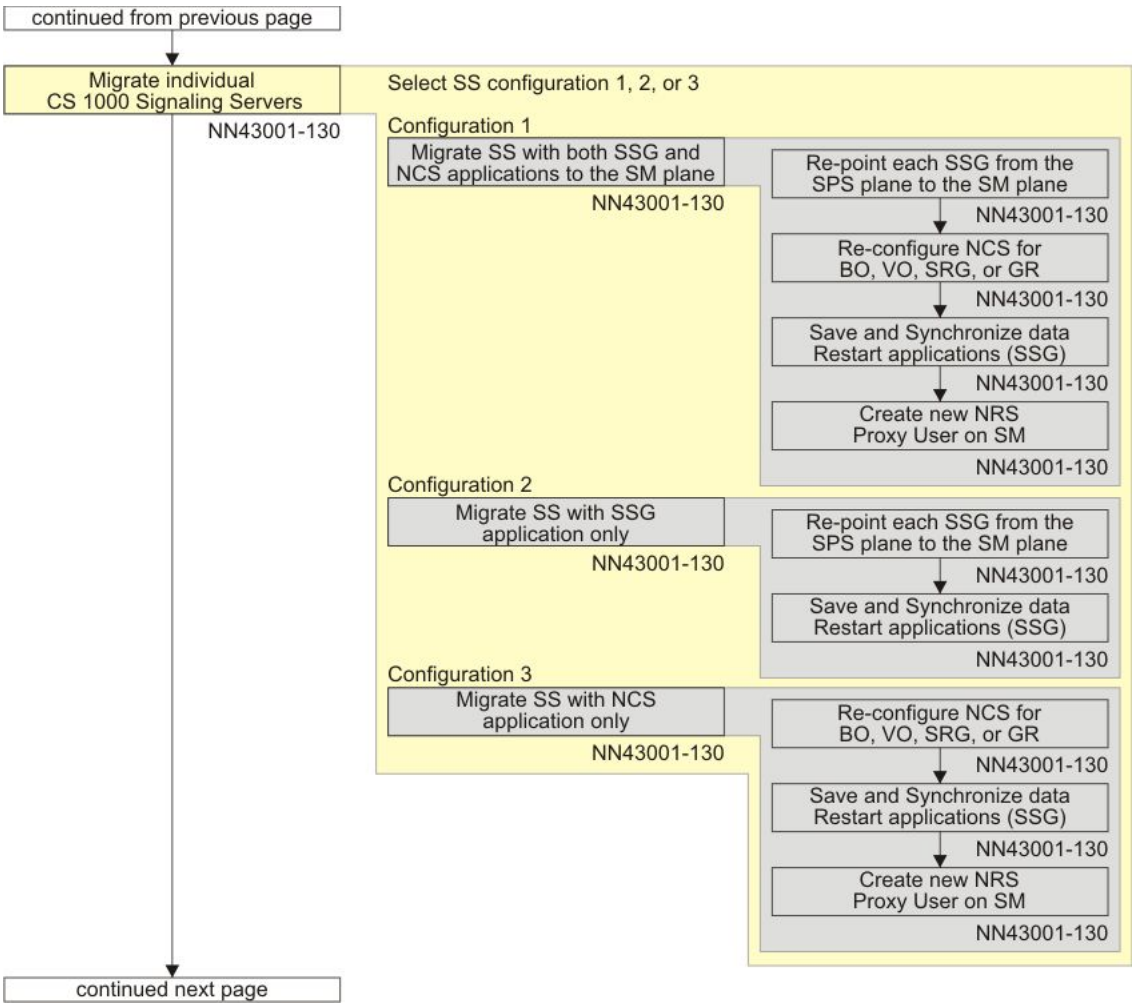

Figure 6: Migration task flow cont

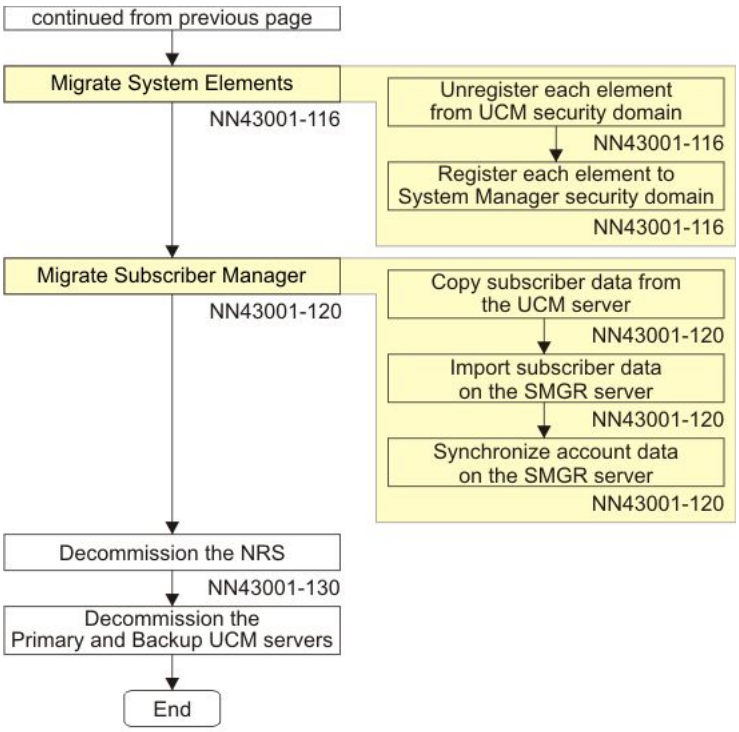

Figure 7: Migration task flow cont

Network Routing Service

Figure 8: Network Routing Service task flow on page 20 appears in *Network Routing Service Fundamentals, NN43001-130*.

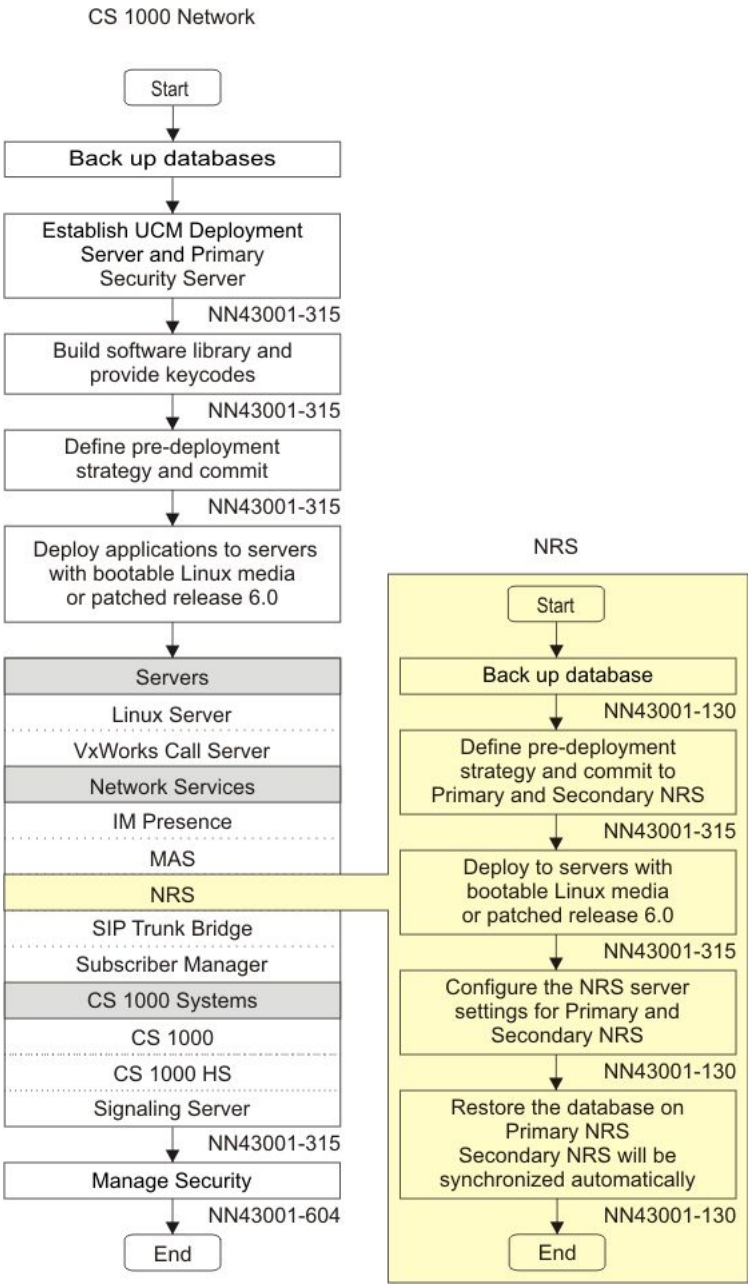

Figure 8: Network Routing Service task flow

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*.

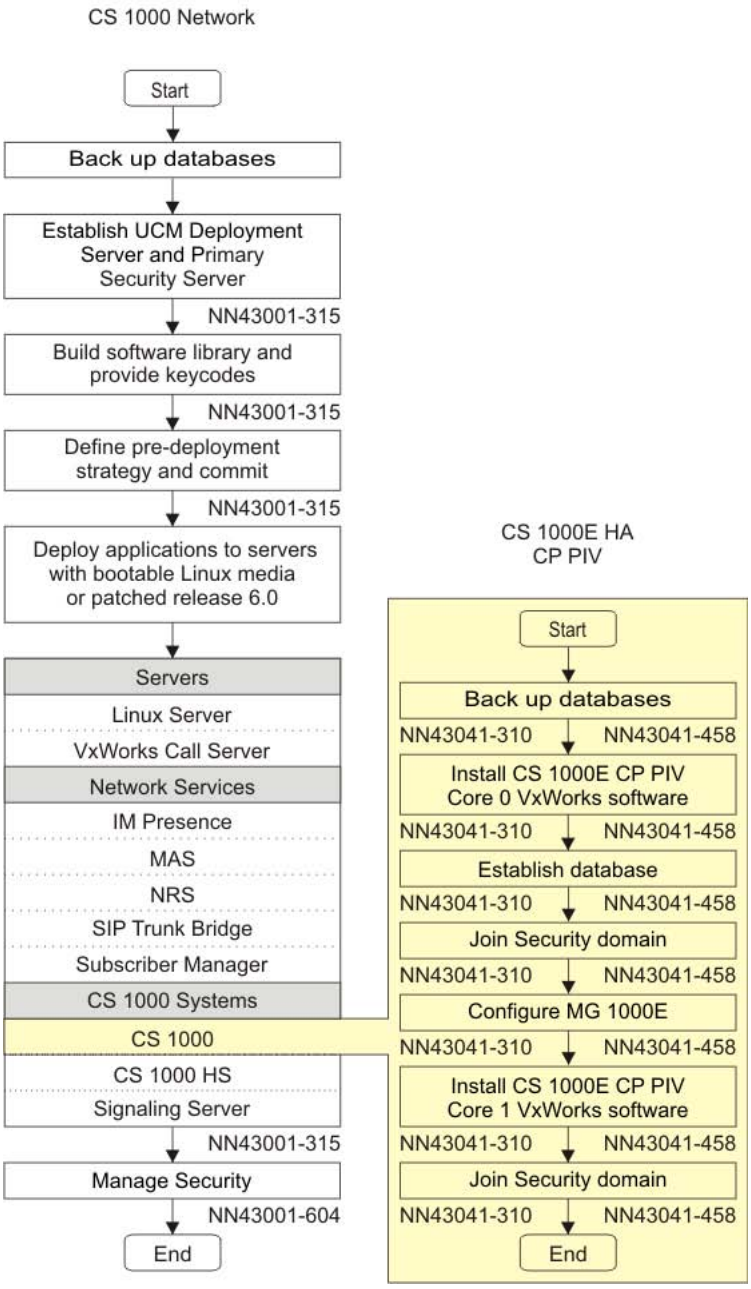

Figure 9: CS 1000E HA CP IV task flow

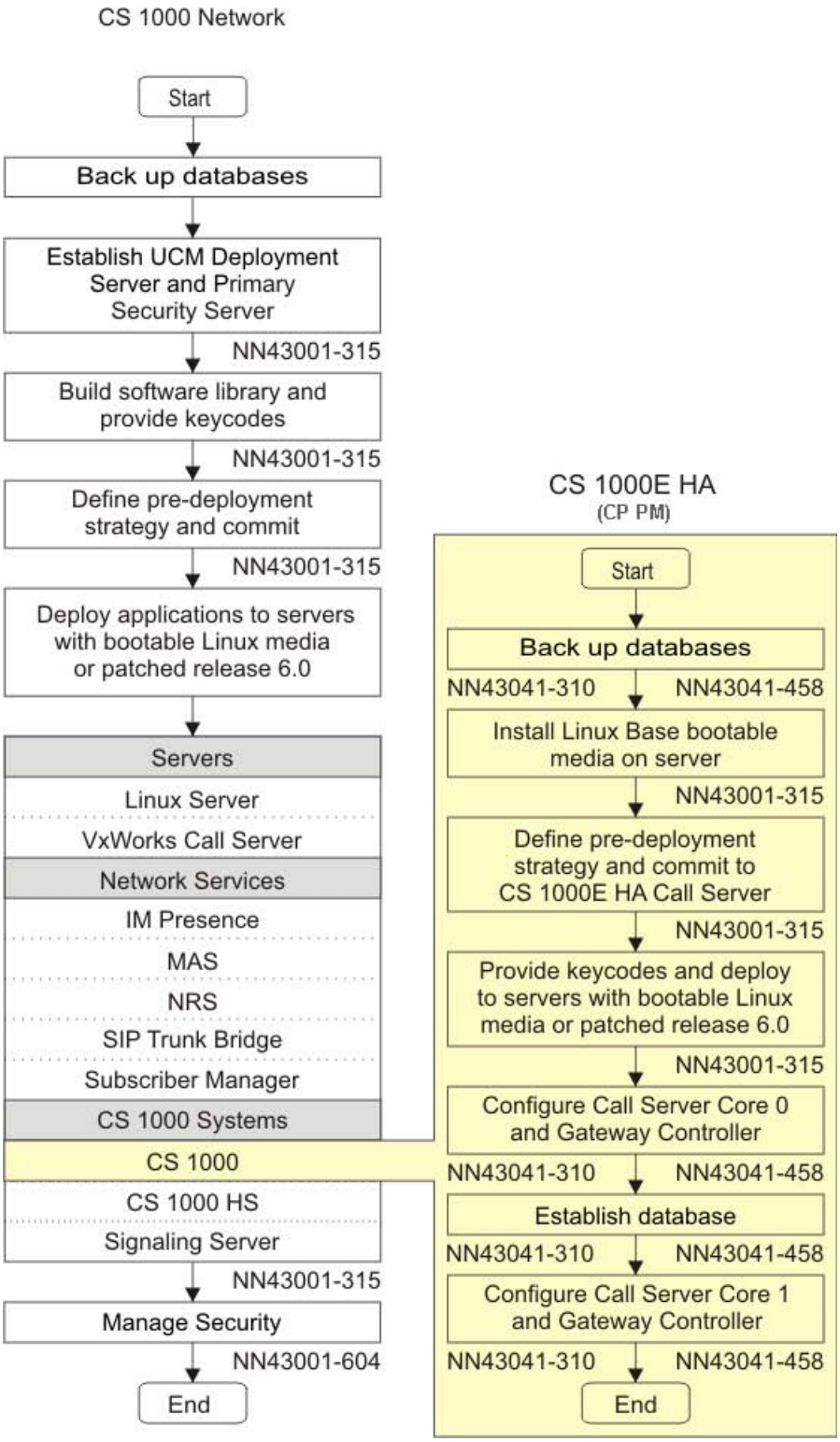

Figure 10: CS 1000E HA CP PM task flow

CS 1000E Co-res

Figure 11: Co-res task flow on page 24 appears in *Co-resident Call Server and Signaling Server , NN43001-509*.

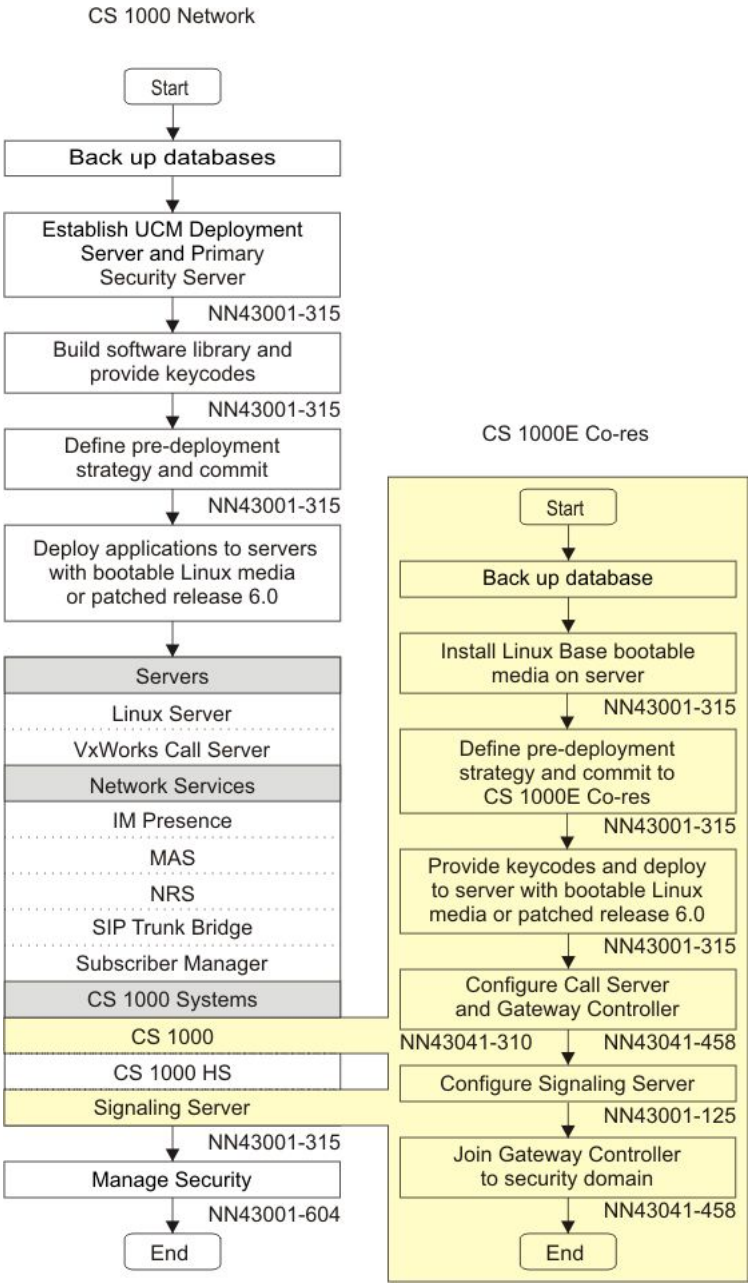

Figure 11: Co-res task flow

CS 1000M

Figure 12: CS 1000M task flow on page 25 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*.

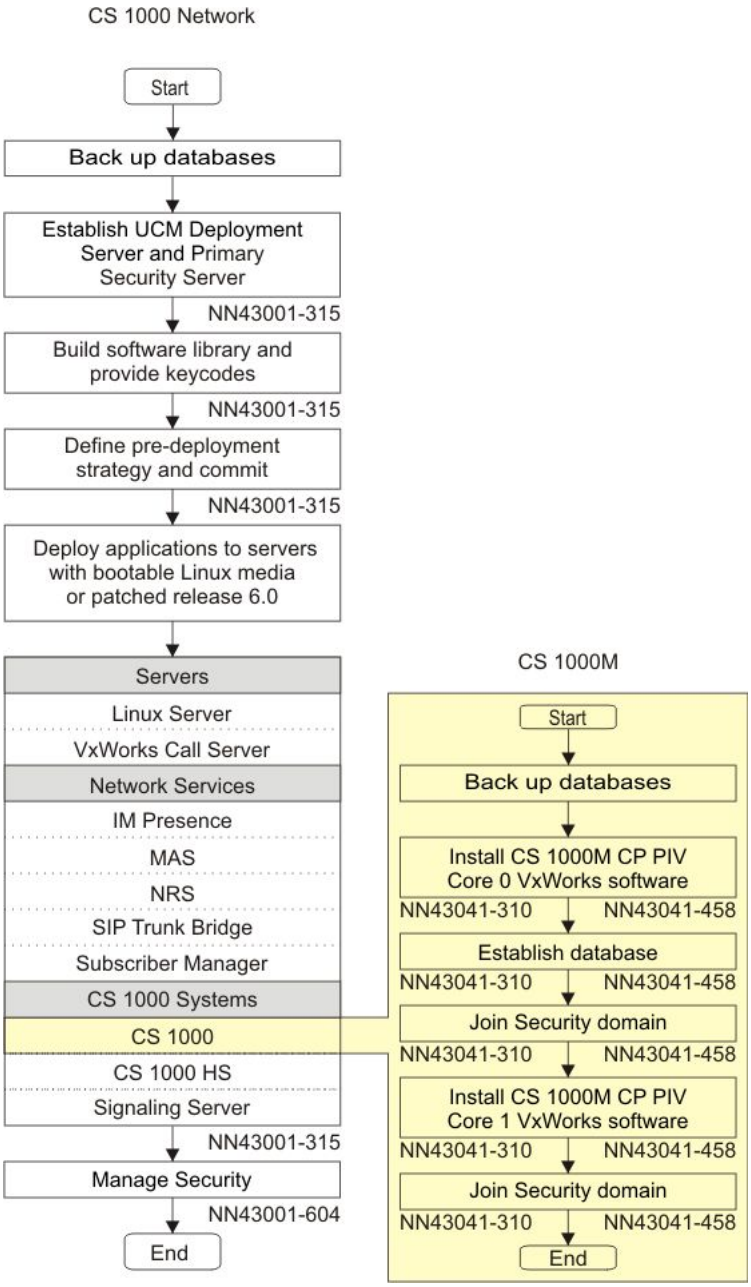

Figure 12: CS 1000M task flow

Signaling Server

Figure 13: Signaling Server task flow on page 26 appears in *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

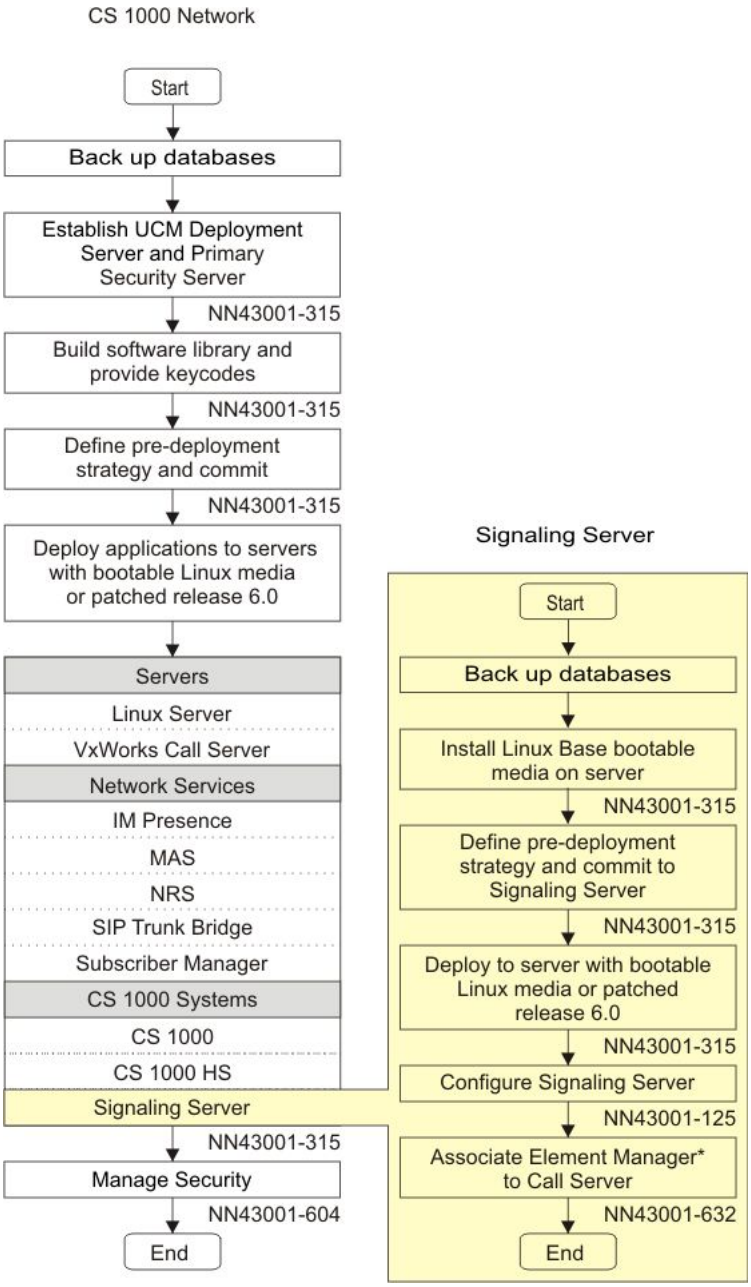

Figure 13: Signaling Server task flow

Branch Office

Figure 14: Branch Office task flow on page 27 appears in *Branch Office Installation and Commissioning , NN43001-314*.

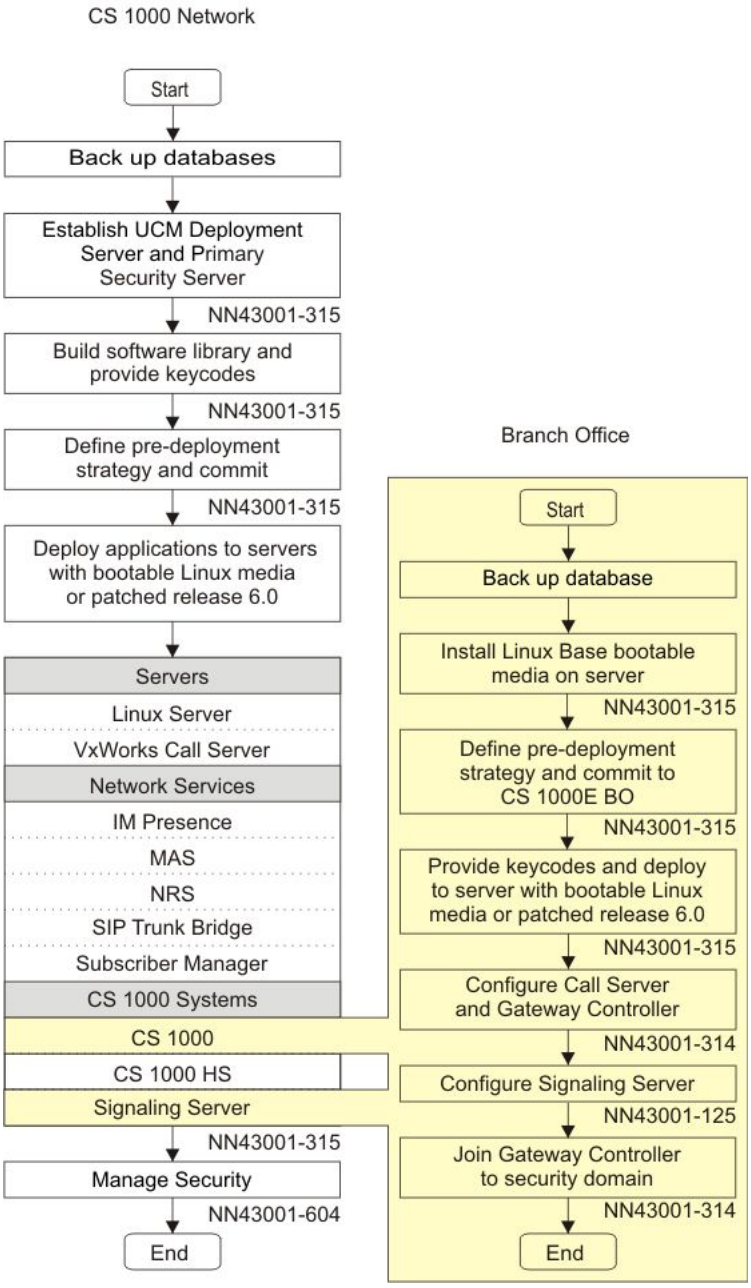

Figure 14: Branch Office task flow

SIP Line

Figure 15: SIP Line task flow on page 28 appears in *SIP Line Fundamentals, NN43001-508*.

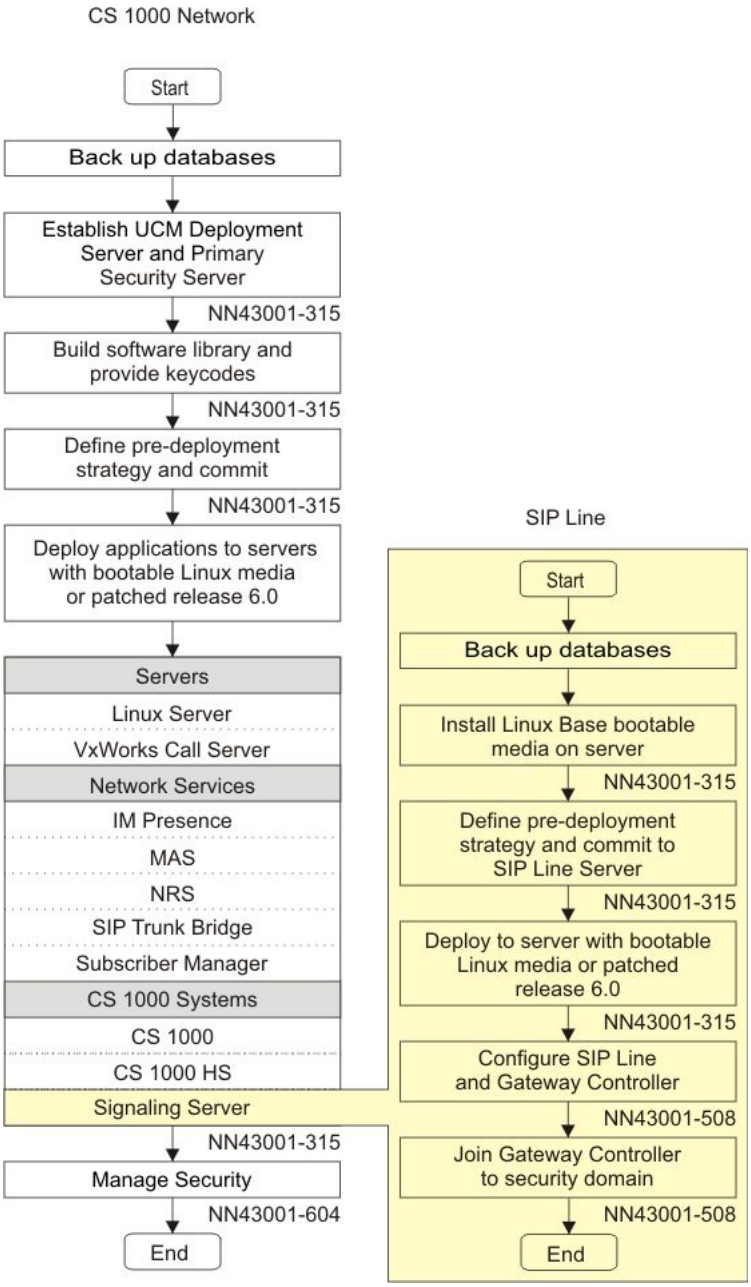

Figure 15: SIP Line task flow

SIP Trunk Bridge

SIP Trunk Bridge appears in *SIP Trunk Bridge Fundamentals , NN43001-143*.

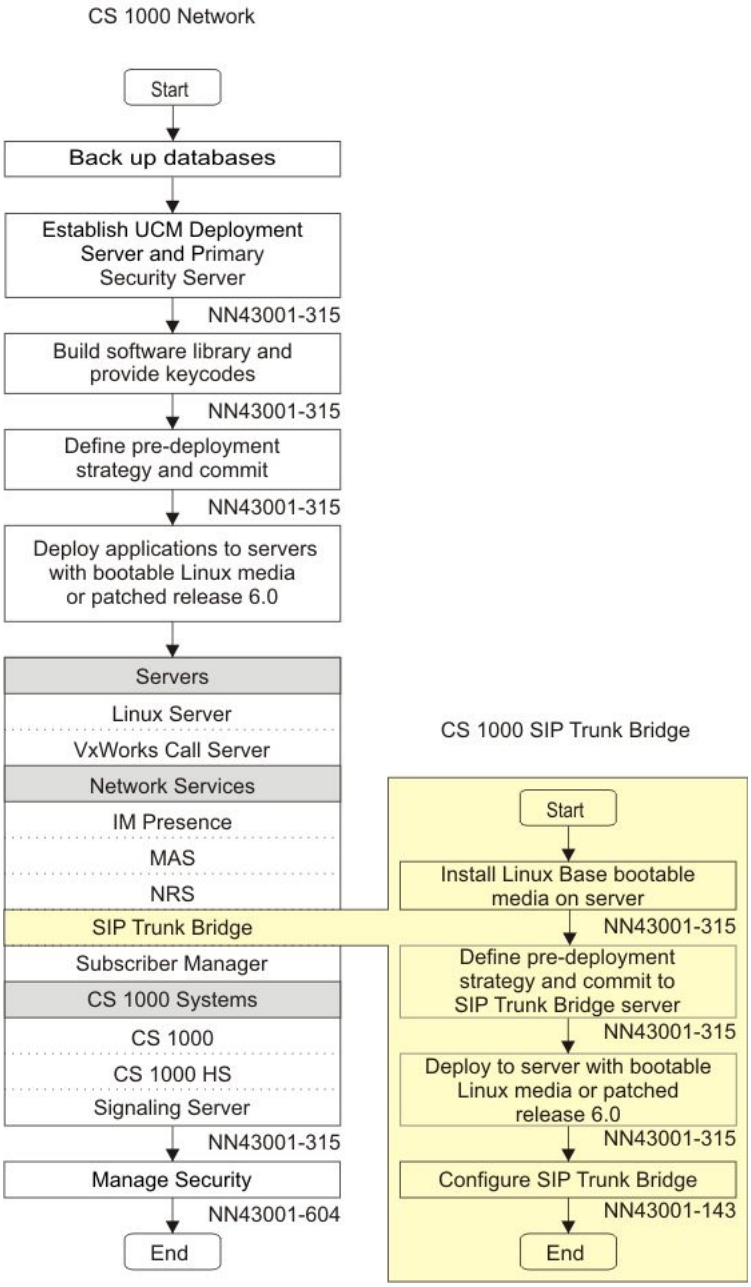

Figure 16: SIP Trunk task flow

High Scalability

Figure 17: High Scalability task flow on page 30 appears in *Communication Server 1000E Planning and Engineering – High Scalability Solutions (NN43041-221)*.

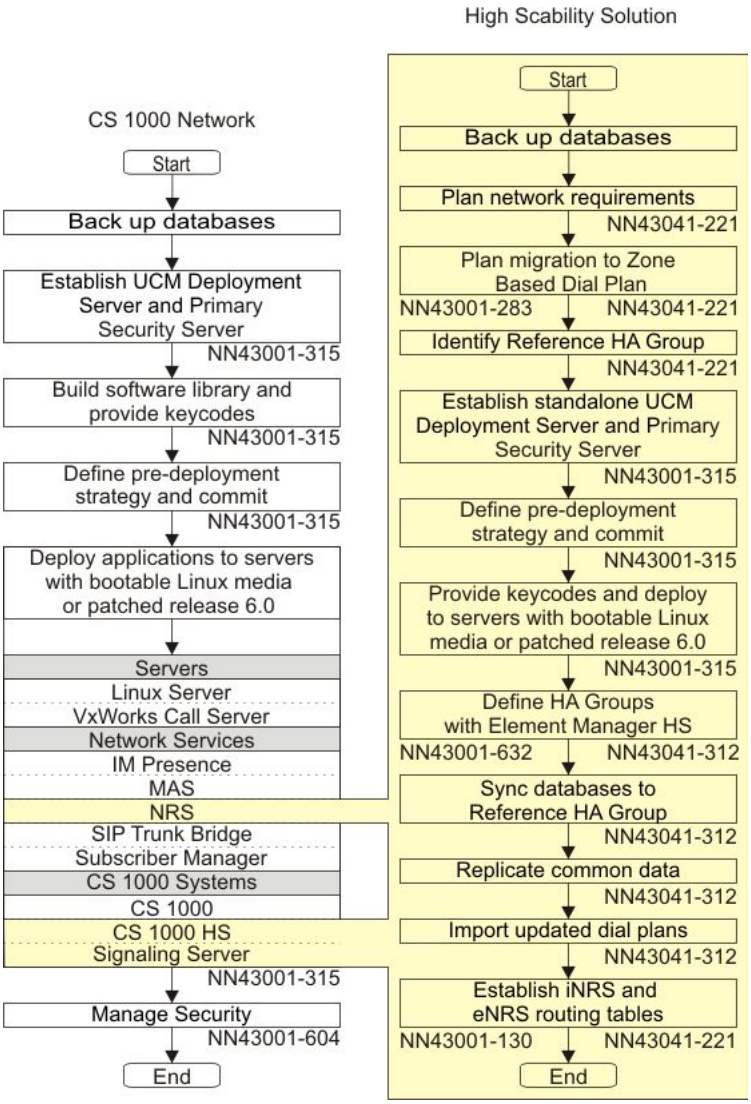

Figure 17: High Scalability task flow

Survivable SIP Media Gateway

Figure 18: Survivable SIP Media Gateway task flow on page 31 appears in *IP Peer Networking Installation and Commissioning , NN43001-313*.

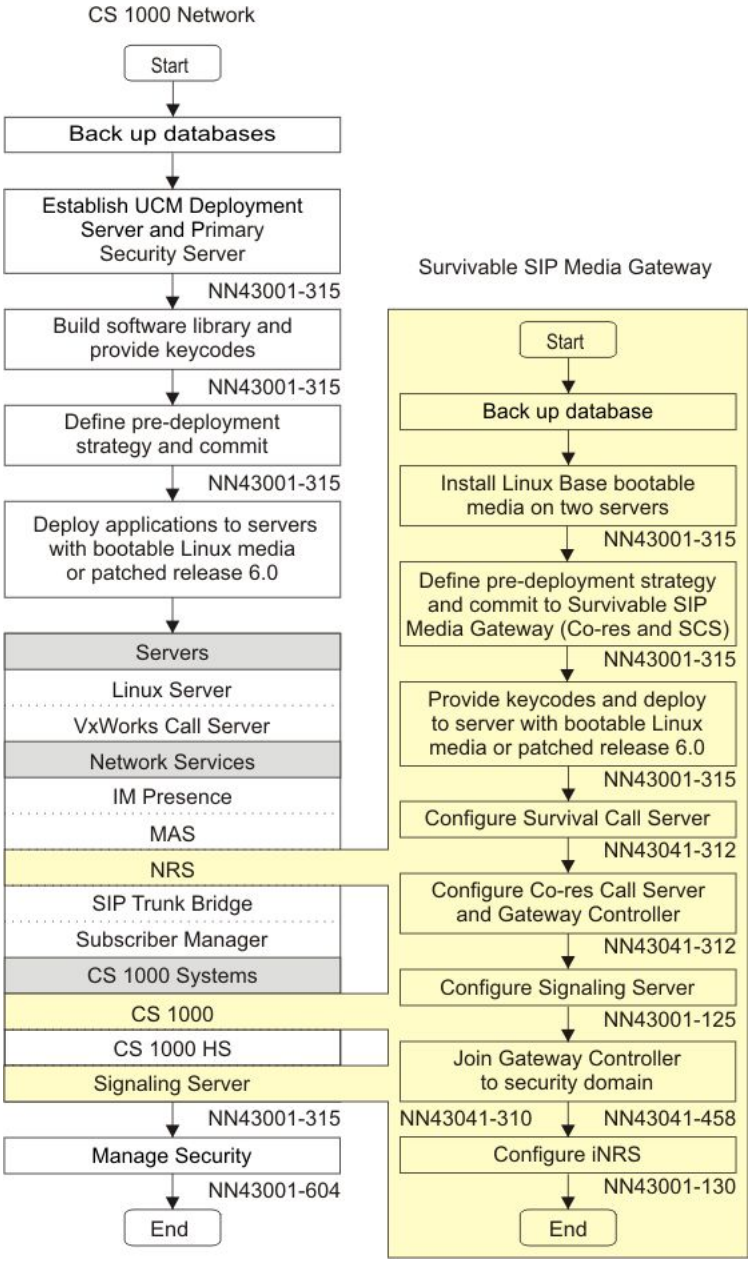

Figure 18: Survivable SIP Media Gateway task flow

Chapter 4: CS 1000 migration to Avaya Aura

Avaya Aura® is the core communications architecture supporting unified communications and contact center solutions for midsize to large enterprises. With CS 1000 Release 7.5, Avaya Aura® extends (rather than replaces) the CS 1000 with revolutionary SIP architecture and virtualization technology. CS 1000 Release 7.5 systems take full advantage of the capabilities of Avaya Aura®, providing faster and easier deployment of communications capabilities such as voice, video, messaging, and presence.

On migrated systems:

- The functionality of UCM has migrated to System Manager, so where this document mentions UCM, interpret it as follows:
  - On systems where System Manager is available, the term UCM refers to System Manager.
  - On systems where System Manager is not available, you can continue to use CS1000/UCM.
- The functionality of NRS/SPS has migrated to Session Manager. A CS 1000 Routing Data Conversion Tool and NRS patches are available to support migration to Session Manager. As a consequence, all statements in CS 1000 technical documents which discuss NRS-SPS dealing with IP Peer Networking are to be construed as references to Session Manager; you now perform SIP Proxy Server configuration using System Manager.
- CS 1000 UCM Data Migration Tool and UCM patches are available to support the migration of the UCM Common Network Directory and Subscriber Manager to System Manager/UCM for CS 1000 7.5 systems.
- NCS functionality has migrated from NRS to Session Manager. As a consequence, all statements in CS 1000 technical documents which discuss NRS-NCS dealing with GR/BO/VO now apply to Session Manager-NCS. You now perform NCS configuration using System Manager.

  For information about the installation and administration of Avaya Aura® Session Manager and System Manager, see the following documents, available at https://support.avaya.com/css/appmanager/css/support:
  - Installing and Upgrading Avaya Aura® System Manager
  - Administering Avaya Aura® System Manager
  - Avaya Aura® Session Manager Overview
  - Installing and Configuring Avaya Aura® Session Manager
  - Administering Avaya Aura® Session Manager

For more information about migrating CS 1000 systems to Avaya Aura®, see *Planning the Network-wide Upgrade* NN43001–406.

Chapter 5: CS 1000 Call Treatment by Aura Session Manager

To provide Aura with information regarding local calls on a CS 1000 Access Element, the Extended Local Calls (ELC) feature routes all local calls to a preconfigured ELC route.

From an end user point of view, ELC calls do not differ from, and are originated in the same manner as, local calls.

When you enable ELC class of service, all local calls for a telephone are routed through ELC SIP trunks if possible. Calls are processed locally only when both parties disable ELC class of service.

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

Chapter 6: Integration of CS 1000 IP Media Services with the Avaya Aura Media Server

Communication Server 1000 Release 7.5 introduces the following changes for IP Media Services:

- Support for proxy mode interaction with Avaya Aura® Session Manager
- Support for MAS clusters using Avaya Aura® Session Manager
- Floating licenses for Avaya MAS 7.0

For more information about IP Media Services, see *Signaling Server IP Line Applications Fundamentals, NN43001–125*.

Chapter 7: Commercial off-the-shelf servers

Overview

The HP Proliant DL360 G7 server is the next iteration of the commercial off-the-shelf (COTS) platform. Server performance is enhanced by more powerful processors (compared to previously introduced COTS servers) and greater memory capacity.

For more information about COTS servers, see *Linux Platform Base and Applications Installation and Commissioning , NN43001-315*.

HP DL360 G7 server specifications

- Intel E5620 Quad core processor (2.4 GHz)
- 146 GB Dual port hard drive, SAS 2.5" form factor, 10 000 RPM
- Base configuration:

  272 total: RAID 5, 3 x 146 GB drive
- Serial attached SCSI
- Three USB ports
- One optical drive
- One USB port in the front, Two USB ports in the back, and one internal USB
- One serial port
- 4 x 1 GB Network Interface Card (NIC) ports

Chapter 8: CS 1000 Element Manager HS completion for serviceability

A High Scalability (HS) system can appear as a single Unified Communications Services and Multimedia Services entity, because the internal High Availability (HA) Groups share a set of common system configuration data, such as Customer, Route, and ESN data blocks. After you update the common data for one HA Group (the reference pair), the updates automatically propagate to the other configured HA groups. With Avaya Communication Server 1000 Element Manager High Scalability (CS 1000 EM HS) you can also bulk provision a new HA Group.

Note:

You must use EM HS to update the common data. Changes that you make by using the command line interface (CLI) do not automatically propagate to the other HA groups.

You can use EM HS to verify the integrity of the automatic update of the common data. You can schedule a daily Common Data Audit or run the audit manually. A scheduled Common Data Audit produces two reports, which provide detailed information about differences or errors in the common data for the HS system. You can easily identify errors; if a report contains errors, the title appears in red text. In the report details, errors appear in red text.

The CS 1000 Element Manager HS completion for serviceability feature also introduces a new Common Data Block type—LD 117, ZONE for Bandwidth Zone.

For more information see *Communication Server 1000E Planning and Engineering — High Scalability Solutions, NN43041-221* and *Communication Server 1000E High Scalability Installation and Commissioning, NN43041-312*.

Chapter 9: IM and Presence application

The Instant Messaging (IM) and Presence application has changed significantly for Communication Server 1000 Release 7.5. As part of the overall integration of Communication Server 1000 to Avaya Aura®, the supported application for IM and Presence has evolved to Avaya Aura Presence Service (PS) Release 6.1.

The implementation of Communication Server 1000 IM and Presence application for Release 6.0 and 7.0 is not supported for Communication Server 1000 Release 7.5. The clients for Release 6.0 and 7.0, IPSP 3456, and the Web tool are no longer supported for Communication Server 1000 Release 7.5.

The Communication Server 1000 Release 7.5 solution for IM and Presence comprises the following four solution elements:

- Avaya Communication Server 1000 Release 7.5 requires the latest DEP list and Service Updates.

  Note:
  Always check the Avaya Support site for the latest versions of the DEP list and Service Updates.

- Avaya Aura Presence Services Release 6.1 is required as the foundational element for Avaya and third-party applications to collect and distribute Presence information an IM capabilities on an enterprise network.
- Avaya System Manager Release 6.1 Service Pack 3 is required. Avaya Aura Presence Services requires System Manager to deploy and manage.
- The specific one-X Communicator 6.1 client for Communication Server 1000 utilizes a Communication Server 1000 SIP Line soft client that is capable of SIP voice and video (point-to-point) services and XMPP-based IM and Presence Services.

The Avaya Aura Presence Services (PS) application requires the XMPP protocol to collect and distribute Presence state information and to deliver Instant Messaging (IM) services. Clients supporting the XMPP protocol are able to participate in the IM and Presence services. The one-X Communicator Communication Server 1000 Release 7.5 client uses the XMPP-capable soft client to deliver SIP voice and video as well as XMPP-based IM and Presence services.

Communication Server 1000 Release 7.5 continues to support tracking of on-the-phone Presence for Communication Server 1000 lines using non-XMPP capable phones and clients. The core Presence Publisher delivers Presence updates to Avaya Aura PS based on provisioning of PREAS Class of Service and implementation of the SIP Converged Desktop ISM for each line to be tracked as in Releases 6.0 and 7.0. Subscriber Manager continues as the management application to define the Presence Services users and is now associated with Avaya System Manager. Subscriber Manager is also used to migrate the Communication Server 1000 users from the previous IM and Presence application to the new Avaya Aura Presence Services.

Chapter 10: PI PEP Integration

Following Product Improvement PEP (PI PEP) are integrated in this release:

- CDR BLID enhancement
- SIP TAT enhancement
- DSC expansion

CDR BLID enhancement

Using this feature you can configure the Call Detail Recording (CDR) such that when a conference or transfer is established between two external DNs, and if the initiator of the call disconnects the line, the initiator's number is printed in the Billing Line Identification (BLID) field in the third line of end record. This is used for billing purpose.

For more information about CDR BLID, see *Call Detail Recording Fundamentals* (NN43001–550).

SIP TAT enhancement

In this feature Trunk Anti Tromboning (TAT) is used to optimize the resources when two DNs are in one of the nodes of Communication Server 1000 and the third DN is in third party SIP client.

For more information about SIP TAT, see *Avaya ISDN Primary Rate Interface Features Fundamentals — Book 3 of 3* (NN43001–569–B3).

DSC expansion

The maximum number if Distant Steering Codes (DSC) are increased to 64000 from 32000.

For more information about DSC, see *Dialing Plans Reference* (NN43001–283).

Chapter 11: Unistim support of G.722 codec

New codec G.722 is introduced in Communication Server 1000E for the UNISTIM 11xx and 12xx IP Phones. Earlier to this release three codec were supported for these IP Phones: G.711, G 723, and G729. Bit rates 64k, 56k, and 48k and payload sizes 10ms, 20ms, 30ms, and 40ms are supported for this new codec.

For more information about G.722 codec, see *Signaling Server IP Line Applications Fundamentals* (NN43001–125).

Chapter 12: SIP ACD for IVR

In Communication Server 1000 Release 7.0, SIP Line provided Interactive Communications Portal (ICP) ports for Interactive Video Response (IVR) using the SIP protocol. However, the Contact Center Offsite Agent (CCOA) and Restricted Agent Observe (RAO) features did not use these SIP Line IVR ports because the SIP IVR feature did not provide login and logout capability on the SIP Line ports.

Contact Center Release 8.0 integrates the CCOA and RAO features with ICP. The CCOA and RAO features can now invoke SIP Line login and logout using the Contact Center Meridian Link Service and Computer Telephony Integration components.

Chapter 13: SIP Line TLS and SRTP support

SIP Line IP Phones and trunks support media security using Secure Real-Time Transport Protocol (SRTP). The Media Security feature allows secure media exchanges on Avaya Communication Server 1000 (Avaya CS 1000) through the use of SRTP on IP media paths.

You can configure the following media security class of service (msec cls):

- Media Security Never (MSNV)
- Media Security Best Effort (MSBT)
- Media Security Always (MSAW)
- Media Security System Defaul (MSSD)

For more information about media security for SIP Line IP Phones, see *SIP Line Fundamentals, NN43001–508*.

Chapter 14: Software Input/Output prompts, responses and commands

Overview

The information in this chapter outlines the new, changed, or retired information in the Software Input/Output Reference documents (NN43001-611) for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.5.

New in this release

The information in this chapter outlines the new or changed information for Communication Server 1000 Release 7.5.

Table 1: Extended Local Calls Prompt and Responses

Prompt	Response	Comment
LD 15 NET Data Block		
ELC	(NO) YES	Extended Local Calls Allowed/Denied
ELC_RLI	0–1999	Route List Index associated to ELC
LD 86 RLB Data Block		
ELC	(NO) YES	Extended Local Calls Allowed/Denied

Table 2: Extended Local Calls Alphabetical List of Prompts

Prompt	Response	Comment	Pack/Rel
LD 10			
CLS	FR2	Fully Restricted 2.	

Prompt	Response	Comment	Pack/Rel
		Note: FR2 restricts access to TIE trunks but allows Extended Local Calls.	basic-7.50
	(ELCD)	Extended Local Calls Denied All incoming and outgoing calls are processed locally when either party is denied Extended Local Calls.	basic-7.50
	ELCA	Extended Local Calls Allowed All incoming and outgoing calls use ELC route.	
LD 11			
CLS	FR2	Fully Restricted 2.	
		Note: FR2 restricts access to TIE trunks but allows Extended Local Calls.	basic-7.50
	(ELCD)	Extended Local Calls Denied All incoming and outgoing calls are processed locally when either party is denied Extended Local Calls.	basic-7.50
	ELCA	Extended Local Calls Allowed All incoming and outgoing calls use ELC route.	
LD 15			
ELC	(NO) YES	Extended Local Calls Allowed/Denied	basic-7.50
ELC_RLI	0–1999	Route List Index associated to ELC	basic-7.50
LD 16			
PCID	xxxx	Protocol ID for the route. Where xxxx: H323 = non-SIP route	basic-2.00
		SIP = SIP route	basic-4.00
		SIPL = SIP Line route	basic-6.00
		SIPE = SIP Extended Local Calls	basic-7.50
LD 86			

Prompt	Response	Comment	Pack/Rel
ELC	(NO) YES	Extended Local Calls Allowed/Denied	basic-7.50

Table 3: IM and Presence Prompt and Responses

Prompt	Response	Comment
LD 11		
PSDN	(NO) YES	CDN used by Presence Publisher as defined in LD 23

Table 4: IM and Presence Alphabetical List of Prompts

Prompt	Response	Comment	Pack/Rel
LD 11			
CLS	(PRED)	Deny Presence service for client.	basic-7.50
	PREA	Allow Presence service for client.	
PSDN	(NO) YES	CDN used by Presence Publisher as defined in LD 23	basic-7.50

Table 5: SRTP support for SIP Lines Prompt and Responses

Prompt	Response	Comment
LD 17		
- MSSD	(MSNV) MSBT MSAW	Media Security Encryption of (MSNV), MSBT, or MSAW. Changing this parameter affects all TNs that have the CLS MSSD.

Table 6: SRTP support for SIP Lines Alphabetical List of Prompts

Prompt	Response	Comment	Pack/Rel
LD 11			
CLS		Media Security Encryption	
	(MSNV)	Media Security Never: Default setting for all users. Implies that there is no attempt to secure either incoming or outgoing calls.	basic-5.00
	MSBT	Media Security Best Effort, Best effort security is attempted for both call originations and terminations.	

Prompt	Response	Comment	Pack/Rel
	MSAW	Media Security Always: strict security option, no incoming or outgoing calls are completed without encryption.	
	MSSD[MSNV]	Media Security System Default (MSNV) as defined by MSSD in LD 17.	basic-7.50
	MSSD[MSBT]	Media Security System Default (MSBT) as defined by MSSD in LD 17.	basic-7.50
LD 17			
MSSD	aaaa	Media Security System Default for TNs as configured in LD11. Where aaaa can equal: (MSNV) Media Security Never MSBT Media security Best Try or “Best Effort” MSAW Media Security Always Secure IP **Note:** Changing this parameter affects all TNs that have the CLS MSSD.	basic-5.00 basic-7.50

New in this release

The following sections detail what’s new in this document for Avaya Communication Server 1000 Release 7.5.

LD 80: Call Trace for Extended Local Calls

VoIP Trace command output

```
Trace command:
.trac 0 79005

Output:

ACTIVE  VTN 120 0 00 05

EXTENDED LOCAL CALL:

ORIG   VTN 120 0 00 05  KEY 0  SCR MARP  CUST 0  DN 79005  TYPE 1230
 SIGNALLING ENCRYPTION: INSEC
 MEDIA ENDPOINT IP: 192.168.30.147  PORT: 5200
TERM   VTN+E1 104 0 13 31   VTRK IPTI  RMBR  19 32 OUTGOING VOIP GW CALL
 FAR-END SIP SIGNALLING IP: 192.168.36.85
 FAR-END MEDIA ENDPOINT IP: 192.168.61.28  PORT: 50002
 FAR-END VendorID: Avaya CS1000 SIP GW release_7.0 version_ssLinux-7.50.07
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  N/A  TXPT  N/A  DIAL DN 79777
MAIN_PM  ESTD
TALKSLOT  ORIG  12   TERM  49
QUEU  NONE
CALL ID 616 19044
---- ISDN ISL CALL (TERM) ----
CALL REF # =  2415
BEARER CAP =  VOICE
HLC =
CALL STATE =  10    ACTIVE
CALLING NO =  79005  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP
CALLED NO  =  79777  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP

ORIG   VTN 104 0 13 00   VTRK IPTI  RMBR  19 1 INCOMING VOIP GW CALL
 FAR-END SIP SIGNALLING IP: 192.168.36.85
 FAR-END MEDIA ENDPOINT IP: 192.168.30.147  PORT: 5200
 FAR-END VendorID: Avaya CS1000 SIP GW release_7.0 version_ssLinux-7.50.07
TERM   VTN 120 0 00 22  KEY 0  SCR MARP  CUST 0  DN 79777  TYPE SLUEXT
 SIGNALLING ENCRYPTION: INSEC
 UEXT PROXY VTN 104 0 14 09   VTRK IPTI  RMBR  3 10 OUTGOING VOIP GW CALL
 FAR-END SIP SIGNALLING IP: 0.0.0.0
 FAR-END MEDIA ENDPOINT IP: 0.0.0.0  PORT: 0
 FAR-END VendorID: Avaya IP Softphone 3456 release 2.6 stamp 57666
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  N/A  TXPT  N/A  DIAL DN 79777
MAIN_PM  ESTD
TALKSLOT  ORIG  24   TERM  29
QUEU  NONE
CALL ID 616 19043
NETWORK  CALL ID  616 19044
---- ISDN ISL CALL (ORIG) ----
CALL REF # =  2614
BEARER CAP =  VOICE
HLC =
CALL STATE =  10    ACTIVE
CALLING NO =  79005  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP
CALLED NO  =  79777  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP
```

Alphabetical list of Call Trace outputs

EXTENDED LOCAL CALL is printed out if call traces are printed for Extended Local Call.

Chapter 15: System messages

System messages are introduced for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.5 in the following message categories:

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

BUG: Software Error Monitor

The following table contains the BUG system messages introduced in Release 7.5.

Table 7: BUG messages

Message	Description	Action	Severity	Monitor	SNMP
BUG0793	ELC Access Ports counter corruption encountered. Counter is reset to ZERO.		Info	NO	NO

ERR: Error Monitor (Hardware)

The following table contains the ERR system messages introduced in Release 7.5.

Table 8: ERR messages

Message	Description	Action	Severity	Monitor	SNMP
ERR0157	There are no more idle ELC Access Ports. Call is processed locally. All ELC Access Ports are busy at this moment. Extended Local Calls cannot be made.	Make sure that you have enough ELC Access Ports configured. Wait until some ELC Access ports will be released.	Minor	YES	YES
ERR0158	CMDB table does not exist.	The table number entered does not exist. Enter a table number that does exist.	Info	NO	NO
ERR0159	Monitor DCH-DSL x for erroneous automated incoming SETUP NCALL messages with invalid digits yyyy. Parameters: x = DCH/DSL number yyyy = DN		Info	NO	NO

ESN: Electronic Switched Network (LD 86, LD 87, and LD 9)

The following table contains the ESN system messages introduced in Release 7.5.

Table 9: ESN messages

Message	Description	Action	Severity	Monitor	SNMP
ESN0122	ELC Route List is intended for ELC	Configure non-ELC Route List	Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
	feature only ELC route list can be used for ELC feature only. Use another route lists for other features.	instead for non-ELC features			
ESN0173	Cannot remove ELC route list. ELC route list (configured in LD15) cannot be removed	Change ELC configuration in Customer Data Block before removing the route list.	Info	NO	NO
ESN0183	ELC prompt value for the route list does not match the route value. You cannot configure an ELC Route in a non-ELC route list.	Configure a corresponding route in the Route List Entry.	Info	NO	NO
ESN0184	Cannot change ELC prompt value. The ELC prompt can not be changed for an existing RLB.	Delete the route list and create a new one.	Info	NO	NO

INFO: Informational messages

The following table contains the INFO system messages introduced in Release 7.5.

Table 10: INFO messages

Message	Description	Action	Severity	Monitor	SNMP
INFO0001	incallDiscMon:The incoming call has been disconnected after it was established for less than x (x: 4 to 10) seconds.		Info	NO	NO

SCH: Service Change

The following table contains the SCH system messages introduced in Release 7.5.

Table 11: SCH messages

Message	Description	Action	Severity	Monitor	SNMP
SCH2410	There are ELCA phones configured. You cannot disable ELC.	Configure ELCD class of service for all phones.	Info	NO	NO
SCH2411	ELC is disabled. ELCA class of service cannot be configured. ELCA class of service can not be configured.	Enable ELC in LD15 before configuring ELCA class of service for a phone.	Info	NO	NO
SCH2413	The number of ELC access ports in the system exceeds the maximum number allowed. You cannot configure additional ELC access ports in LD14.		Info	NO	NO
SCH2414	The ELC route list is intended for the ELC feature only. You cannot configure an ELC route list for a non-ELC feature.	Configure a non-ELC route list instead.	Info	NO	NO
SCH2415	The route list is not intended for Extended Local Calls.	Provide the ELC route list Index for the ELC_RLI prompt.	Info	NO	NO
SCH2416	SIP Extension of local calls cannot be configured if NARS or FNP is disabled. Extended local calls feature cannot be configured.	Enable NARS and FNP.	Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
SCH2417	The route cannot be removed or changed. The specified route is configured in a RLB or another data block.	Remove all references to the route from all data blocks.	Info	NO	NO
SCH2418	ISM limit of IP Music connections (IP MUS CON) is equal to 0. The IP Music connections (IP MUS CON) ISM limit equals 0 and cannot be decremented.		Warning	NO	NO
SCH2419	ISM limit of IP Media Sessions is equal to 0. The IP Media Sessions ISM limit equals 0 and cannot be decremented.		Warning	NO	NO
SCH2420	The UC password cannot be configured because the PUID has not been configured.	Configure the PUID first.	Minor	NO	NO
SCH2421	You must configure the UC Password (UPWD) for SIP Line.	Configure the UC Password for SIP Line.	Minor	NO	NO
SCH2422	IP Media Services package not equipped.		Warning	NO	NO
SCH2423	CMDB table does not exist.	The table number entered does not exist. Enter a table number that does exist.	Info	NO	NO
SCH2424	Extended Local Calls feature does not support this phone type.		Info	NO	NO

SYS: System Loader

The following table contains the SYS system messages introduced in Release 7.5.

Table 12: SYS messages

Message	Description	Action	Severity	Monitor	SNMP
SYS0186	The number of IP Peer ELC Trunks exceeds the IP Peer ELC Trunks ISM limit and no further IP Peer ELC Trunks can be sysloaded.		INFO	NO	NO
SYS0187	Media Security is turned off because DME (423) package is unrestricted. Media Security was found to be enabled in a configuration record during sysload. It must be disabled because the Disable Media Encryption package is equipped.	Ensure the keycode file is valid and the DME package is unrestricted legitimately.		YES	YES

TFS: Traffic Measurement

The following table contains the TFS system messages introduced in Release 7.5.

Table 13: TFS messages

Message	Description	Action	Severity	Monitor	SNMP
TFS0005	IP Tone could not be connected because ISM limit was reached.		Warning	NO	NO
TFS0006	IP Conference could not be established		Warning	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
	because ISM limit was reached.				