Planning the Network-wide Upgrade Avaya Communication Server 1000

7.5
NN43001-406, 05.09
September 2011

© 2011 Avaya Inc.

All Rights Reserved.

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: New in this release 5
- Feature changes 5
- Other changes 6

Chapter 2: Customer service 7
- Navigation 7
- Getting technical documentation 7
- Getting product training 7
- Getting help from a distributor or reseller 7
- Getting technical support from the Avaya Web site 8

Chapter 3: Introduction 9
- Subject 9
- Note on legacy products and releases 9
- Applicable systems 9
  - System migration 9
- Intended audience 10
- Terminology 10
- Related information 12
  - Publications 12
  - Online 12

Chapter 4: Software requirements 13
- Main office and Branch Office running the same release 13
- Main office and Branch Office running different releases 13
  - Features in mixed-software configuration 14
  - Adding a Branch Office to an existing network 14
- Main office requirements 15
  - Optional features 16
- Branch Office requirements 16
- Main office and Branch Office 17
- Main office to main office - peer interworking 18
- Main office to Branch Office - peer interworking 19
- Geographic redundancy 20
  - Geographic redundancy operation 20
- Avaya CS 1000 Release 7.5 compatibility matrix 21
- Interoperability with other products 21

Chapter 5: Planning considerations for the network-wide upgrade 27
- Contents 27
- Introduction 27
- Planning for a new platform 27
- CS 1000 migration to Avaya Aura® System Manager 28
- UCM 39
- Network Routing Service 39
- System and network level security 40
  - Security domain 40
  - Security domain considerations and guidelines 41

Central and local authentications ... 42
Intra-System Signaling Security or IPsec ... 42
Datagram Transport Layer Security ... 44
Network Time Protocol configuration ... 45
Deployment considerations ... 46
Management of IP telephony nodes ... 46
Personal directory and unicode name directory ... 47
Primary and secondary NRSs ... 47
Element manager ... 47
Primary and secondary UCM security servers ... 48
Subscriber Manager ... 49
Survivable Remote Gateway ... 49
Chapter 6: Upgrading the IP telephony network ... 51
UCM ... 52
Complete upgrade to UCM ... 52
Gradual upgrade to UCM from ECM ... 56
NRS or SPS ... 57
Survivable Remote Gateway ... 58
CS 1000M ... 59
CS 1000E ... 59
Avaya MG 1000E ... 59
Media cards ... 59
Signaling server ... 61
Avaya MG 1000B ... 61
Security settings ... 61
Setting loadware ... 61
Index ... 63

Chapter 1: New in this release

The following sections details what's new in *Planning the Network-wide Upgrade* (NN43001-406) for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.5.

Navigation

- Feature changes on page 5
- Other changes on page 6

Feature changes

UCM/NRS functionality in System Manager/Session Manager 6.1

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 are available in System Manager. You must migrate existing systems with a Network Routing Service (NRS) to Session Manager (some exceptions apply). 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 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.

For information about migration to Avaya Aura®, see CS 1000 migration to Avaya Aura® System Manager on page 28.

Other changes

There are no other changes in this document

Revision history

September 2011	Standard 05.09. This document is up-issued to include updates to the migration to Avaya System Manager and Session Manager content.
June 2011	Standard 05.06. This document is up-issued to include updates to security domain content.
November 2010	Standard 05.05. This document is up issued to support Communication Server 1000 Release 7.5.
November 2010	Standard 05.04. This document is published to support Communication Server 1000 Release 7.5.
November 2010	Standard 05.03. This document is published to support Communication Server 1000 Release 7.5.
November 2010	Preliminary 05.01–05.02. This document is issued to support Communication Server 1000 Release 7.5.
June 2010	Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.0.
July 2009	Standard 03.17. This document is up issued to reflect changes made to section Planning considerations for the network-wide upgrade.
June 2009	Standard 03.16. This document is issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.15. This document is issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.14. This document is issued to support Communication Server 1000 Release 6.0.
December 2007	Standard 02.02. This document is issued to support Communication Server 1000 Release 5.5.
May 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0. No new content has been added for Communication Server 1000 Release 5.0. All references to Communication Server 1000 Release 4.5 are applicable to Communication Server 1000 Release 5.0.

Comments? infodev@avaya.com

Chapter 2: 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 on page 7
- Getting product training on page 7
- Getting help from a distributor or reseller on page 7
- Getting technical support from the Avaya Web site on page 8

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 3: Introduction

This 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 includes the following information:

- provides the necessary information for a network administrator to plan a total network upgrade
- identifies the software releases required for the upgrade

Note on legacy products and releases

This publication contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 (Avaya CS 1000) software. For more information about 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)

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 6.0 software and configured to include a Signaling Server, they become CS 1000M systems.The following table lists each Meridian 1 system that supports an upgrade path to a CS 1000 Release 7.5 system.

Table 1: Meridian 1 systems to CS 1000 Release 7.5 systems

This Meridian 1 system...	Maps to this CS 1000 Release 7.5 system
Meridian 1 PBX 11C Chassis	CS 1000E
Meridian 1 PBX 11C Cabinet	CS 1000E
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81C	CS 1000M Multi Group

For more information, see one or more of the following publications:

- *Communication Server 1000M and Meridian 1 Small System Software-only Upgrade* (NN43011-459)
- *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)
- *Communication Server 1000E Software Upgrades* (NN43041-458)

Intended audience

This document is intended for individuals responsible for planning a network upgrade.

Terminology

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

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

In this document, the following hardware is referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Expander chassis (NTDK92) - legacy hardware
- Option 11C Cabinet (NTAK11) - legacy hardware
- MG 1000E Chassis (NTDU14) and Expander chassis (NTDU15)
- MG 1010 Chassis (NTC310)
- IPE module (NT8D37) with MG XPEC card (NTDW20)

In this document, the following hardware platforms are referred to generically as Server:

- Call Processor Pentium IV (CP PIV) card
- Common Processor Pentium Mobile (CP PM) card

- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
  - IBM x360m server (COTS)
  - HP DL320 G4 server (COTS)
  - IBM x3350 server (COTS2)
  - Dell R300 server (COTS2)

In this document, the following cards are referred to generically as Gateway Controller:

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)

The following table shows CS 1000 supported roles for common hardware platforms.

Table 2: Hardware platform supported roles

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP IV	yes	no	no	no
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	yes	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS	no	yes	no	no
COTS2	no	yes	yes	no

Note:
The CP MG card functions as a Server and the Gateway Controller while occupying slot 0 in a chassis, cabinet, and MG 1010.

For information about CP MG, see *Linux Platform Base and Applications Installation and Commissioning*, NN43001-315.

Related information

This section lists information sources that relate to this document.

Publications

The following documents are referenced in this document:

- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *SIP Line Fundamentals* (NN43001-508)
- *Security Management Fundamentals* (NN43001-604)
- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Product Compatibility Reference* (NN43001-256)
- *Dial Plans Reference* (NN43001-283)
- *IP Peer Networking Installation and Commissioning* (NN43001-313)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *System Management Reference* (NN43001-600)
- *Emergency Services Access Fundamentals* (NN43001-613)
- *Telephones and Consoles Fundamentals* (NN43001-567)
- *ISDN Primary Rate Interface Fundamentals* (NN43001-569)
- *Basic Network Feature Fundamentals* (NN43001-579)
- *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)
- *Communication Server 1000E Software Upgrades* (NN43041-458)

Online

To access Avaya documentation online, go to http://www.avaya.com/support.

Chapter 4: Software requirements

This chapter describes the relative software versions required in the Main office and Branch Office locations. The actual software packaging requirements are given in Main office requirements on page 15 and Branch Office requirements on page 16. It contains information on the following topics:

- Main office and Branch Office running the same release on page 13
- Main office and Branch Office running different releases on page 13
- Main office requirements on page 15
- Branch Office requirements on page 16
- Main office and Branch Office on page 17
- Avaya CS 1000 Release 7.5 compatibility matrix on page 21
- Interoperability with other products on page 21

Main office and Branch Office running the same release

Normally, the main office and associated Branch Office run the same software release.

However, a Branch Office location can be running an earlier software release than that running at the main office. This situation is discussed in the following section.

Main office and Branch Office running different releases

Ensure that the software release on the Branch Office matches the software release on the main office. The main office Call Server and the Branch Office can have different software releases, as long as the main office runs the higher release. For example, with the main office running Avaya Communication Server 1000 (Avaya CS 1000) Release 6.0 software the Branch Office must run Communication Server 1000 Release 6.0, Release 5.5, or Release 5.0.

CS 1000 supports a mixed Main/Branch Office combination where the Branch Office can run software that is one releases older than the Main Office – this configuration is approved for continued use:

- Main Office at Release 7.5 MG1000B can be on Release 7.5, 7.0 or 6.0
- Main Office at Release 7.0 MG1000B can be on Release 7.0 or 6.0

- Main Office at Release 6.0 MG1000B can be on Release 6.0, 5.5, or 5.0
- Main Office at Release 5.5 MG1000B can be on Release 5.5, 5.0, 4.5, or 4.0

CS 1000 supports a mixed Main/Branch Office combination where the Branch Office can run software that is two releases older than the Main Office – this configuration is recommended only for temporary use during upgrades:

- Main Office at Release 7.5MG1000B can be on Release 5.5 or 5.0
- Main Office at release 7.0 MG1000B can be on Release 5.5 or 5.0
- Main Office at release 6.0MG1000B can be on Release 4.5 or 4.0
- Main Office at release 5.5MG1000B can be on Release 3.0

Important:

Both the Call Server and Signaling Server in the main office must run the same release of software. Upgrade the Branch Office Communication Server 1000 within thirty days, to the same Avaya CS 1000 release installed on the main office.

Important:

If the NRS at the Branch Office is also the Alternate NRS in the network, then both Alternate and the Primary NRS must be running the same software release.

For information on upgrading an existing main office and associated its Branch Offices, see *Branch Office Installation and Commissioning* (NN43001-314).

Features in mixed-software configuration

IP Deskphone users in Normal Mode use the feature set on the main office. IP Deskphone users in Local Mode use the feature set on the Branch Office. Users of analog and digital devices always use the feature set on the Branch Office.

If the Branch Office is running a lower release of software than the main office, features involving interaction between the main office and the Branch Office do not function for the Branch Office IP Deskphone users. For example, if the main office is on Communication Server 1000 Release 7.0 and the Branch Office is on Communication Server 1000 Release 5.0 or 5.5, features introduced in Avaya CS 1000 Release 7.0 are not available for the Branch Office IP Deskphone users, because these features are not supported on earlier releases.

Adding a Branch Office to an existing network

Customers who want to add a Branch Office to their existing network can order a Branch Office running an older CS 1000 release, if their main office is running that release. For example, you can order a Branch Office running Communication Server 1000 Release 5.0 if your main office is running Communication Server 1000 Release 5.0.

Comments? infodev@avaya.com

Important:

Both the Call Server and Signaling Server in an office must run the same release of software. The Main office must always run the highest software release on the Call Server and the Signaling Server.

Important:

A main office running CS 1000 Release 4.0, CS 1000 Release 4.5, or CS 1000 Release 5.0 software does not support a Branch Office running CS 1000 5.5 or later software.

Important:

If the NRS at the Branch Office is also the Alternate NRS in the network, then both alternate and the primary NRS must be running the same release of software.

Main office requirements

The Branch Office feature requires IP Peer H.323 Trunk (H323_VTRK) package 399. This package is required to support H.323 functionality. Overlap Signaling (OVLP) package 184 is included with package 399.

Important:

The main office must have a software Service Level of 2 or higher to work with the Branch Office.

The main office requires the following software packages to support the specified Basic Network features. For more information, see *Basic Network Feature Fundamentals* (NN43001-579).

- Network Call Back Queuing (NCBQ) package 38. This package is required for SRG IP Deskphones to invoke any queuing feature or Ringback When Free feature.
- Network Speed Call (NSC) package 39. This package is required for SRG IP Deskphones to invoke the Network Speed Call feature.

The main office requires the following software packages to support the specified ISDN Primary Rate Interface features. For more information, see *ISDN Primary Rate Interface Fundamentals* (NN43001-569).

- Network Attendant Service (NAS) package 159 -- This package is required for analog (500/2500-type) telephones in the Branch Office to access attendant services when the attendant is configured on the main office.
- Network Message Services (NMS) package 175 -- This package is required for analog (500/2500-type) telephones in the Branch Office to share the voicemail system in the main office. For any configurations using centralized Avaya CallPilot on the main office with one or more Branch Offices in separate time zones, the NMS package is required at the main office for the branch IP Deskphones.

Optional features

- Network Alternate Route Selection (NARS) package 58. For more information, see *Basic Network Feature Fundamentals* (NN43001-579).
- Overlap Signaling (OVLP) package 184.This package is optional; it is required for overlap signaling. It is packaged with H.323 Virtual Trunk (H323_VTRK) package 399 (Release 4.0 and Release 4.5).
- Emergency ServicesAccess (ESA) package 329.This package is optional and is required to receive 911/ESA features. For more information, see *Emergency Services Access Fundamentals* (NN43001-613).
- Virtual Office (VIRTUAL_OFFICE) package 382 and Avaya 3900 Digital Deskphone Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387. These packages are optional; they are required only for Virtual Office functionality.
- Network Signaling (NSIG) package 37. This package is optional for SRG IPDeskphones to access set-based Network Class of Service (NCOS) features.
- Adaptive Network Bandwidth Management package 407.
- Alternate Routing for Network Bandwidth Management.
- SIP Gateway and Converged Desktop (SIP) package 406. This package is optional; it is required to support SIP functionality.

Branch Office requirements

The Branch Office feature requires the hardware. For more information about specific hardware requirements, see *Branch Office Installation and Commissioning* (NN43001-314). The MG 1000B Call Server also requires the following software packages:

- Command Status Link (CSL) package 77
- Integrated Services Digital Network (ISDN) package 145
- Flexible Numbering Plan (FNP) software package 160. For more information, see *Dialing Plans Reference* (NN43001-283).
- Overlap Signaling (OVLP) package 184.This package is required only if overlap signaling is to be implemented in the Branch Ofice. For more information, see *IP Peer Networking Installation and Commissioning* (NN43001-313).
- Enhanced ACD Routing (EAR) package 214
- Enhanced Call Trace (ECT) package 215
- Emergency Services Access (ESA) package 329

Comments? infodev@avaya.com

- Virtual Office (VIRTUAL_OFFICE) package 382 and Avaya 3900 Digital Deskphone Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387. These packages are optional; they are required only for Virtual Office functionality.
- BMG package 390
- IP Peer H.323 Trunk (H323_VTRK) package 399. This package is optional; it is required for H.323 functionality. The packaging for package 399 also includes package 184.

Important:

These packages are automatically enabled in the Branch Office software.

The Branch Office feature also requires the SIP Gateway and Converged Desktop (SIP) package 406 for SIP. This package may or may not be automatically enabled in the Branch Office software, depending on the region in which the software is used.

When using Set-Based Installation at the MG 1000B, install the following:

- Set Relocation (SR) package 53
- Flexible Feature Code (FFC) package 139
- Automatic Installation (AINS) package 200

The feature packages listed above are automatically enabled in the Branch Office software.

If the main office is equipped with Location Code Expansion (LOCX) package 400, the Branch Office must also have this package. For more information, see *ISDN Primary Rate Interface Fundamentals* (NN43001-569).

Important:

The key codes used to install software at the Branch Office differ from those used to install software at the main office.

Main office and Branch Office

This section describes the existing rules for software release compatibility between main office and Branch Offices. It is possible for a main office Call Server and the Branch Office MG 1000B to temporarily have different software releases, if the main office is running the later release.

By allowing this mixed software operation, customers do not have to upgrade their entire network of Branch Offices in order to add a single additional Branch Office running the most recent CS 1000 software. This permits the network upgrade to be scheduled over a longer period. The main office Call Server must be running the latest CS 1000 software release. Issues within a release are considered equivalent.

The features available to IP Deskphone users in Normal mode is the feature set on the main office. In Local mode, the IP Deskphones use the feature set of the Branch Office. Analog (500/2500-type) or digital telephones always use the feature set of the Branch Office.

If the main office Call Server is running CS 1000 Release 4.0 software, the following rules apply:

- Branch Offices can run CS 1000 Release 4.0 or Succession Release 3.0 Software permanently.
- The Branch Office can temporarily run CS 1000 Release 2.0 software.This is required to support customers who are currently running a network of CS 1000 Release 2.0 branch systems, and who want to add one branch (running CS 1000 Release 4.0 software).
- A mix of CS 1000 Release 2.0, Succession Release 3.0, and CS 1000 Release 4.0 Branch Offices is not allowed at any time.

If the main office Call Server is running Succession Release 3.0 Software, the following rules applies:

- Branch Offices can only run Succession Release 3.0 Software on a permanent basis. No permanently mixed software configurations are allowed.
- The Branch Office can temporarily run CS 1000 Release 2.0 software.This is required to support customers who are currently running a network of CS 1000 Release 2.0 branch systems, and who want to add one branch (running Succession Release 3.0 Software). It enables customers to migrate the network gradually.
- Branch Offices cannot run CS 1000 Release 4.0 software or later.

If the main office Call Server is running CS 1000 Release 2.0 software, the following rule applies:

Branch Offices can only run Succession Release 2 software. No mixed software configurations are allowed.

IP Deskphones do not download software from the main office. IP Deskphones download their software from the Branch Office. Therefore, an IP Deskphone running firmware for Succession Release 3.0 can be connected to a main office running CS 1000 Release 4.0. For more information about Branch Office, see *Branch Office Installation and Commissioning* (NN43001-314).

Main office to main office - peer interworking

Table Table 3: Peer interworking - main office to main office on page 19 shows the peer interworking between any combinations of the software releases 7.5, 7.0, 6.0, 5.5, 5.0, 4.5, 4.0, and 3.0.

Comments? infodev@avaya.com

Table 3: Peer interworking - main office to main office

Software Releases	7.5	7.0	6.0	5.5	5.0	4.5	4.0	3.0
7.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
7.0	X	Supported	Supported	Supported	Supported	Supported	Supported	Supported
6.0	X	X	Supported	Supported	Supported	Supported	Supported	Supported
5.5	X	X	X	Supported	Supported	Supported	Supported	Supported
5.0	X	X	X	X	Supported	Supported	Supported	Supported
4.5	X	X	X	X	X	Supported	Supported	Supported
4.0	X	X	X	X	X	X	Supported	Supported
3.0	X	X	X	X	X	X	X	Supported

Main office to Branch Office - peer interworking

A mixed Main or Branch combination is supported where the Branch can be:

- one release back for continued usage or on a permanent basis
- two releases back for the upgrade path only on a temporary basis

Table Table 4: Branch - one release back on page 19 shows supported Mixed Main/Branch combinations for Branch that is one release back:

Table 4: Branch - one release back

Main office Release	MG1000B	MG1000B supported release
6.0	Supported	6.x, 5.x
5.5	Supported	5.x, 4.x

Table Table 5: Branch - two releases back on page 20 shows supported Mixed Main or Branch combinations for Branch that is two releases back:

Table 5: Branch - two releases back

Main office Release	MG1000B	MG1000B supported release
6.0	Supported	4.x
5.5	Supported	3.x

Geographic redundancy

Geographic redundancy (GR) uses a GR N-Way database replication model that allows the main office and Geographic redundancy man office (GRMO) to use the same database without manual replication. Any Branch Office SIP set should be able to register through the Branch Office, the main office, or the GRMO, depending on the failover case.

Important:

Only GR 1+1 is supported. GR N+1 is not supported.

The GR SIP Line Gateway sends keep alive messages regularly and they are a critical decision maker in case of any incoming registration or calls based on the background keep alive mechanism.

There are two approaches to support GR for SIP Line clients: S1/S2 configuration or DNS configuration. Not all clients support S1/S2 configuration, both the S1/S2 solution and the DNS solution are offered in GR operation. This option is chosen on a per SIP Line Gateway basis.

Geographic redundancy operation

The operation from a main office client point of view in an S1/S2 configuration:

- Client configuration
  - main office client S1 – pointing to GR SLG
  - main office client S2 – pointing to Main SLG
- Normal operation
  - Client tries registration with GR SLG (S1)
  - GR SLG maintains status of main office
  - GR SLG redirects client to main office SLG
- Main office down
  - Client tries registration with GRS SLG (SL1)

Comments? infodev@avaya.com

- GR SLG maintains status of main office, client stays at GR

• Main office comes back

GR SLG redirects client to main office SLG

Avaya CS 1000 Release 7.5 compatibility matrix

For compatible applications that operate with Avaya CS 1000 Release 7.5 software, obtain the CS 1000 Release 7.5 product Bulletin or contact your Avaya distributor before upgrading. Compatibility information is also available to distributor partners through the Partner Information Center at http://www.avaya.com

For information about card compatibility, see *Product Compatibility Reference* (NN43001-256).

Interoperability with other products

Consult your documentation for compatibility matrices which apply to earlier versions of software to ensure that any upgrades of the auxiliary processors remain compatible with the versions of software in your network. Ensure that compatible applications are always running during the upgrade process, unless service interruptions are acceptable.

Table 6: Interoperability with other products

Product	Release
Call Server	
CS 1000 N-1, N-3 CS1K	Release 4.5 and 5.5
CS 2100 (SIP, H.323, PRI)	SE11
MCS5100/MAS	MCS 4.0
BCM50	Release 3.0
BCM450	Release 1.0
CS 2000	CVM11
Branch Office	
SRG50	Release 3.0
Avaya Aura	
Avaya Aura Session Manager	Release 6.1
Avaya Aura System Manager	Release 6.1

Product	Release
Applications	
ACE(Agile Communication Environment)	Release 1.1
MPS 500	3.0.0.15
MPS IP (Avaya NES ICP)	1.0.1.155
Avaya NES Contact Center	Release 6.0
NMC	Release 6.0
AG(1000/2000)	Release 6.3
Messaging	
HMS400	Release 2.0
Avaya CallPilot	Release 5.0
Microsoft Exchange UM2007	SP1
UM2000	Release 3.3
3rd Party Partner Products	
Microsoft OCS2007	Wave 12
AudioCodes M2K/M1K	Release 5.2
T-Metric Attendant Console	Release 6.0
Data	
SMC	Release 1.1
Clients	
Mobile X	As included with CS 1000 lineup
Teledex	As included with CS 1000 lineup
MC3100	Release 3.0 SU 123
SIP Clients (11xx, 68xx, 1535)	As included with CS 1000 lineup
SIP DECT	FW 4910b416
Competitive	
Cisco Call Manager	Release 6.0

Table 7: Release comparison summary

Auxiliary Processors	Succession Release 3.0	CS 1000 Release 4.0
Attendant consoles		
PC Attendant Console	1.2.x	1.2.x

Comments? infodev@avaya.com

Auxiliary Processors	Succession Release 3.0	CS 1000 Release 4.0
Avaya 2250 Attendant Console	Supported	Supported
SMILE	2.3.x	2.3.x
Digital Deskphones		
Avaya 39xx Digital Deskphones	F/W version shipped with Release 3.0	F/W version shipped with Release 4.0
Meridian Modular Telephones (M2xxx)	Supported	Supported
ITG-P and Media Cards		
IP Line	3.1	4.0
IP Trunk	3.00.53, 3.01.22, 3.01.60 (Will resolve with Signaling Server 2.10.81, 2.11.03, 4.00.xx.)	3.01.22, 3.01.60 (Will resolve with Signaling Server 2.11.03, 4.00.xx.)
System management		
Optivity Telephony Manager (OTM)	OTM 2.1 and OTM 2.2	OTM 2.2
Element Manager	Part of core Signaling Server software	Part of core Signaling Server software
Messaging		
Avaya CallPilot	1.07 (with Service Update 4), 2.0 Used on Platforms: 201i, 702t, 703t, 1001rp, 1002rp versions	1.07 (with Service Update 4), 2.0, 2.5 Used on Platforms: 201i, 702t, 703t, 1001rp, 1002rp versions
HMS 400	1.0	1.0
Avaya CallPilot Mini	1.5, 1.5A, 1.5B, 1.5C, 1.5D Small Systems only	1.5, 1.5A, 1.5B, 1.5C, 1.5D Small Systems only
Meridian Mail Modular Option EC	12.12-13.14	12.12-13.14
Meridian Mail Enhanced Card Option	12.12-13.14	12.12-13.14
Meridian Mail Reporter R2.X	Not dependent on core software	Not dependent on core software
Wireless		
Companion	3.xx -7.xx (7.xx required for Enhanced Capacity)	3.xx -7.xx (7.xx required for Enhanced Capacity)
Voice over Internet Protocol (VoIP)		

Auxiliary Processors	Succession Release 3.0	CS 1000 Release 4.0
Meridian DECT (DMC4/ DMC8 version)	451000.xx / 470001.xx – software embedded on IPE card	451000.xx / 470001.xx – software embedded on IPE card
VoIP – 802.11 Wireless IP Gateway with Symbol	Application supported on ITG Pentium only 1.1x	Application supported on ITG-P 24-port card 1.19, 1.20
Avaya 2001 IP Deskphone	Not supported	Firmware version shipped with Release 4.0
Avaya 2002 IP Deskphone	Firmware version shipped with Release 3.0	Firmware version shipped with Release 4.0
Avaya 2004 IP Deskphone	Firmware version shipped with Release 3.0	Firmwareversion shipped with Release 4.0
IP Phone 2002 Phase II	Not supported	Firmware version shipped with Release 4.0
IP Phone 2004 Phase II	Not supported	Firmware version shipped with Release 4.0
Avaya 2050 IP Softphone	Firmware version shipped with SR3.0	Firmware version shipped with Release 4.0
WLAN Handset 2210/2211	Not supported	Firmware Release 97.039
IP Telephony Manager 2245	174.007	174.007
Remote office portfolio		
Remote Office 9150	1.3.1, 1.3.4, 1.4.x, 1.5.x	1.4.x, 1.5.x
Remote Office 9110/9115/ IP Adaptor	1.3.1, 1.3.4, 1.4.x, 1.5.x	1.4.x, 1.5.x
Meridian Home Office MHO-II	1.18 Not supported with Avaya 3900 Digital Deskphone Phase III	1.18 Not supported with Avaya 3900 Digital Deskphone Phase III
Mini Carrier Remote	Supported	Supported
Carrier Remote	Supported	Supported
Fiber I	Supported	Supported
Fiber II	Supported	Supported
Remote Peripheral Equipment (RPE)	Not supported	Not supported
Retired call center applications		
Meridian MAX (any platform)	(9.2, 9.3), 10.x	Not supported

Comments? infodev@avaya.com

Auxiliary Processors	Succession Release 3.0	CS 1000 Release 4.0
Network Administration Center (NAC)	Not supported - End of Life Last release - 2.5	Not supported
Meridian Customer Controlled Routing (MCCR)	Not supported - End of Life Last release - 3B, 3C	Not supported
Meridian Link (Mlink)	Not supported - End of Life Last release - 5, 5C	Not supported
Symposium Link	Not supported	Not supported
Symposium Desktop TAPI Service Provider for Meridian Communicator Adapter (MCA)	Not supported - End of Life Last release - 1.x - 2.x	Not supported
Meridian Link & MCCR Co-residency	Not supported	Not supported
Symposium Call Center and CTI applications		
Symposium Telephone Application Programming Interface (TAPI) Service Provider	2.3.1, 3.0	3.0
Symposium Agent	2.3	2.3
Symposium Agent Greeting	2.0	2.0
Remote Agent Observe	1.0	1.0
Meridian Link Services (MLS)	4.2	5.0
Symposium Express Call Center (SECC)	4.2	4.2
Symposium Call Center Server (SCCS) **Important:** Includes Symposium Web Client	4.0, 4.2, 5.0	4.2, 5.0
Symposium Web Centre Portal (SWCP)	4	4.0
CTI.next (Communications Control Toolkit)	5.0	5.0
IVR applications		
Periphonics IVR (VPS/is)	5.x	5.x

Auxiliary Processors	Succession Release 3.0	CS 1000 Release 4.0
Periphonics Integrated Package for Meridian Link (IPML) – VPS/is and MPS	2.0.x, 2.1	2.0.4, 2.0.5, 2.1
Periphonics Multimedia Processing Server (MPS) 100	1.0, 2.1	1.0, 2.1
Periphonics Multimedia Processing Server - MPS 500, MPS 1000	2.1	2.1
Periphonics Integrated Package for Meridian Link (IPML) – MPS 500, MPS 1000	2.1	2.1
Avaya Business Communications Manager		
Avaya Business Communications Manager	3.5	3.5, 3.6
Survivable remote gateway	1.0	1.0
NNIXX portfolio		
Integrated Call Assistant	1.05 and above	1.5
Integrated Conference Bridge (NNICB)	2.1x, 3.xx	2.1, 3.0x, 4.0
Integrated Recorded Announcer	2.0.16 and above	2.0.16 and above
Integrated Personal Call Director	1.0.3 and above	1.0.3 and above, 2.0
Hospitality Integrated Voice Services	1.17	1.17
MCS 5100		
MCS 5100	1.1	2.0, 3.0
Communication Server 2000		
CS 2000	SN06.2	Not supported
Avaya CS 2100	SE06.2	Not supported

Chapter 5: Planning considerations for the network-wide upgrade

Contents

This chapter contains information on the following topics:

- Introduction on page 27
- Planning for a new platform on page 27
- UCM on page 39
- Network Routing Service on page 39
- System and network level security on page 40

Introduction

This section describes what combinations of mixed software are allowed in a network running Avaya Communication Server 1000 (Avaya CS 1000). Mixed situations are likely to occur temporarily as the upgrade progresses.

Planning for a new platform

Select a suitable platform for each of the signaling servers.This requires planning for ordering hardware.

- IP addressing schemes
- IP addressing scope
- Host naming
- FQDN
- ELAN/TLAN
- Firewalls

CS 1000 migration to Avaya Aura® System Manager

Avaya CS 1000 Release 7.5 offers complete Avaya Aura® integration.

Avaya Aura® is the core communications architecture supporting unified communications and contact center solutions for midsize to large enterprises. Avaya Aura® extends the Avaya Communication Manager and enables SIP-based session management with innovative capabilities, and with CS 1000 Release 7.5, Avaya Aura® also 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® architecture, providing faster and easier deployment of communications capabilities such as voice, video, messaging, and presence.

To migrate a CS 1000 system to Avaya Aura® System Manager and Session Manager, you must migrate the CS 1000 core components (such as media gateways and call servers), as well as each instance of the following components to the System Manager domain:

- Network Routing Servers (NRS)
- SIP Proxy Servers
- SIP Line Servers
- SIP Signaling Gateways
- Geographically Redundant Branch Office

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/UCM.
  - On systems where System Manager is not available, continue to use CS 1000/ UCM.
- 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 R7.5 systems.
- The functionality of NRS/SPS has migrated to Session Manager. A CS 1000 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.
- 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.

Comments? infodev@avaya.com

- After migration, you can continue to use NRS if you require any of the following:
  - During migration of NRS to SM for multi-site customers
  - H.323 trunks
  - IPv6
  - IP Attendant console (Direct connect to gateway IP is supported)
  - Internal NRS for CS 1000E HS configuration
- The following settings are not retained by the migration tool and must be reconfigured after migration:
  - IPsec—disable IPsec before migration.
  - SNMP
  - Numbering Groups
  - Passwords—migration provides the default password policy, which you can modify if required.

For information about the installation and administration of Avaya Aura 6.1 Session Manager and System Manager, see the following documents 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

Migrating Other CS 1000 SIP Solution Components

CS 1000 SIP solutions typically consist of a number of SIP-enabled components, in addition to CS 1000 SIP Signalling Gateways, that used the CS 1000 NRS/SPS routing services in the past. For example, Avaya SRG.

Before you migrate a CS 1000 SIP solution from NRS SIP-based core to Session Manager SIP-based core, consult the CS 1000 Release 7.5 interoperability with other products to confirm that these additional solution components satisfy the SIP interoperability requirement with Session Manager R6.1. For more information about the CS 1000 Release 7.5 Interoperability with other products, see Interoperability with other products on page 21.

Network Routing Service Fundamentals NN3001–130 describes how to administer NRS-related parameters. The same administration steps apply to migrated solutions, except that you complete NRS steps using the System Manager/Session Manager interface.This means, for example, that you must administer the IPaddress and SIPtransport and port of the Session Manager instead of the NRS.

If any non-CS 1000 components that use the functionality of the NRS are connected to your system, see the *CS 1000 Release 7.5 Product Compatibility Matrix NN43001-141* to confirm that they are compatible with Session Manager 6.1. Ensure that any components that are not compatible do not register to Session Manager.

The following table provides information about NRS to Session Manager migration rules and policy.

Table 8: NRS to Session Manager Rules/Policy

CS 1000 Release 7.5 NRS to Session Manager Rules/Policy	May Maintain NRS	Require to Migrate to Session Manager
IPv6	Yes	No
H.323 Trucking	Yes	No
IP Attendant console	Yes	No
CS 1000 High Scalability (Internal NRS only)	Yes (Internal NRS)	Yes* (external NRS replaced by Session Manager)
MS OCS R2 with TLS/sRTP	Yes	No
MS Exchange UM2007	Yes	No
During migration NRS to Session Manager for multi-site customers	Yes	Yes*
MG 1000B/SRG with H.323 trunking and Unistim IP Phones	Yes	No
MG 1000B/SRG with SIP trunking and Unistim or SIP IP Phones	No	Yes*
SMG 1000E with H.323 trunking and Unistim or SIP IP Phones	Yes	No
SMG 1000E with SIP trunking and Unistim IP Phones	No	Yes*
SMG 1000E with Unistim IP Phones and no SIP trunking	Yes	No
Survivable SIP Media Gateway or SIP Media Gateway	No	Yes*
Secure Router 2330/4131	No	Yes*
* Denotes that Quality Framework is required – http://porteal.avaya.com/ptlWeb/service/SV0555 Notes: If migrating NRS to SM for R6.0 and above, then also required to migrate UCM to System Manager. For software releases R5.5 and earlier, required to upgrade to R7.5 to be supported with Avaya Aura 6.1		

Comments? infodev@avaya.com

CS 1000 migration to Avaya System Manager and Session Manager task flow diagrams

This section provides two high level task flows for migrating CS 1000 systems to Avaya System Manager and Session Manager.

- Option One: For R4.x – R7.0 CS 1000 systems that have upgraded to CS 1000 R7.5 prior to migrating to Avaya System Manager and Session Manager.
- Option Two: For R4.x – R7.0 CS 1000 systems that are migrating to Avaya System Manager and Session Manager before upgrading the CS 1000 Call Servers and registered elements to R7.5.

Option One requirements:

- CS 1000 UCM must be on a standalone server platform. System Manager does not support running NRS, EM, or Call Server. System Manager supports the following CS 1000 services:
  - Deployment Manager
  - Patch Manager
  - Subscriber Manager
  - Secure FTP Token
  - SNMP
  - IPSec—If IPSec is enabled to the CS 1000 UCM primary, it must be disabled prior to migration. System Manager does not support IPSec to itself. System Manager does support configuring IPSec to the other CS 1000 components.
- UCM backup server is not supported. System Manager does not support a backup server.
- ELAN and TLAN must be routable. System Manager only supports one Ethernet port therefore it must have access to both ELAN and TLAN. The current best practice is to connect System Manager to ELAN, ensuring TLAN is routable.

Option Two requirements:

- NRS Migration Patch required for R5.x – R7.0.

  Note:
  Release 4.x NRS database cannot be migrated to Session Manager.
- Access to CS 1000 Data Conversion Tool at https://nrstool.avaya.com/default.aspx

Task flows

Each task flow indicates the recommended sequence of events to follow when configuring a system and provides the number of the technical document that contains the detailed procedures required for the task.

- For information about migrating UCM, see the *Unified Communications Management Common Services Fundamentals NN43001–116*.
- For information about migrating the NRS to System Manager, see the *Network Routing Service Fundamentals NRS NN43001–130*.
- For information about migrating Subscriber Manager, see the *Subscriber Manager Fundamentals NN43001–120*.

Option One task flow

The following three figures provide the CS 1000 Option One migration to System Manager (SMGR) and Session Manager (SM) task flow.

Comments? infodev@avaya.com

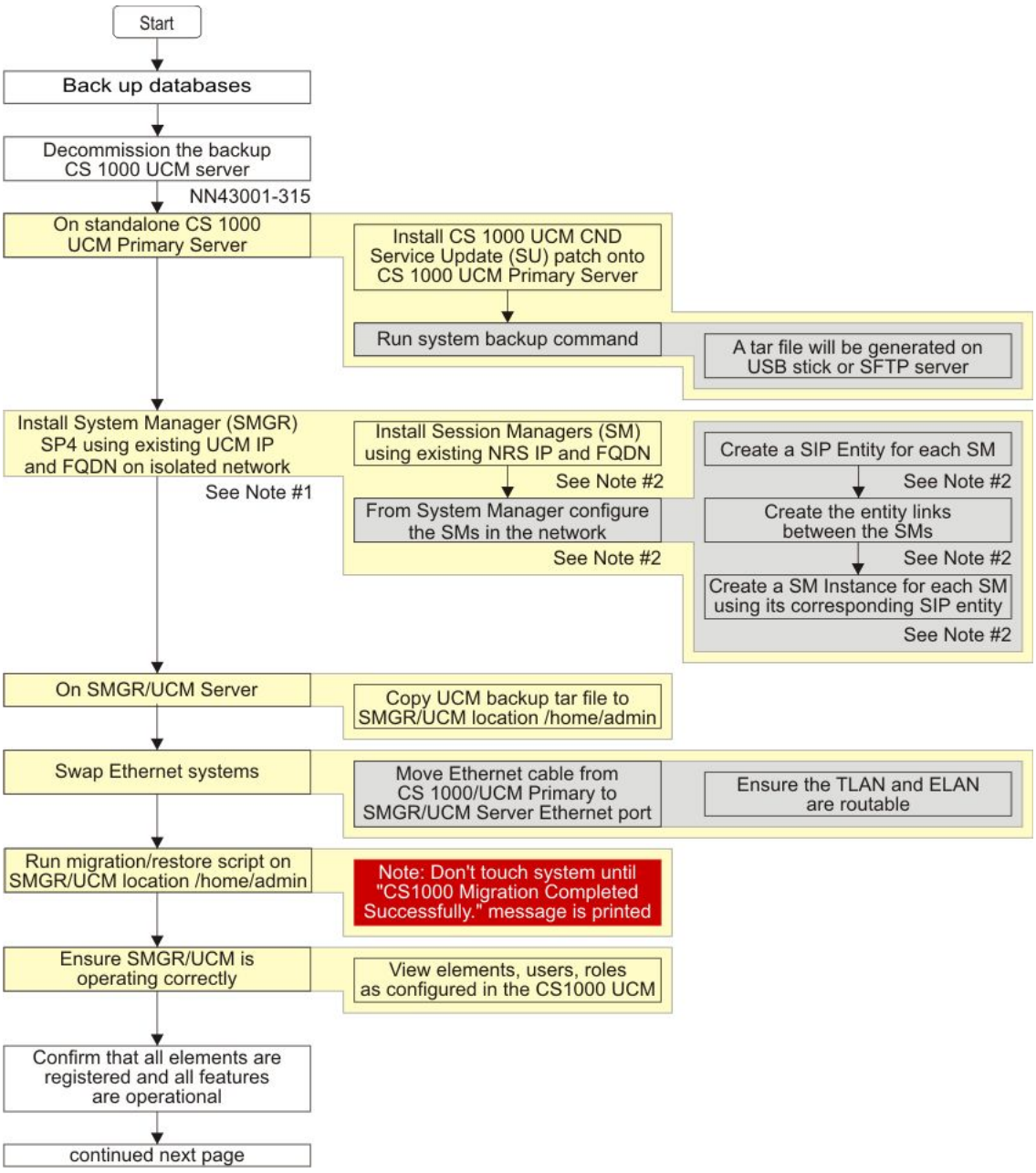


Figure 1: Option One task flow 1

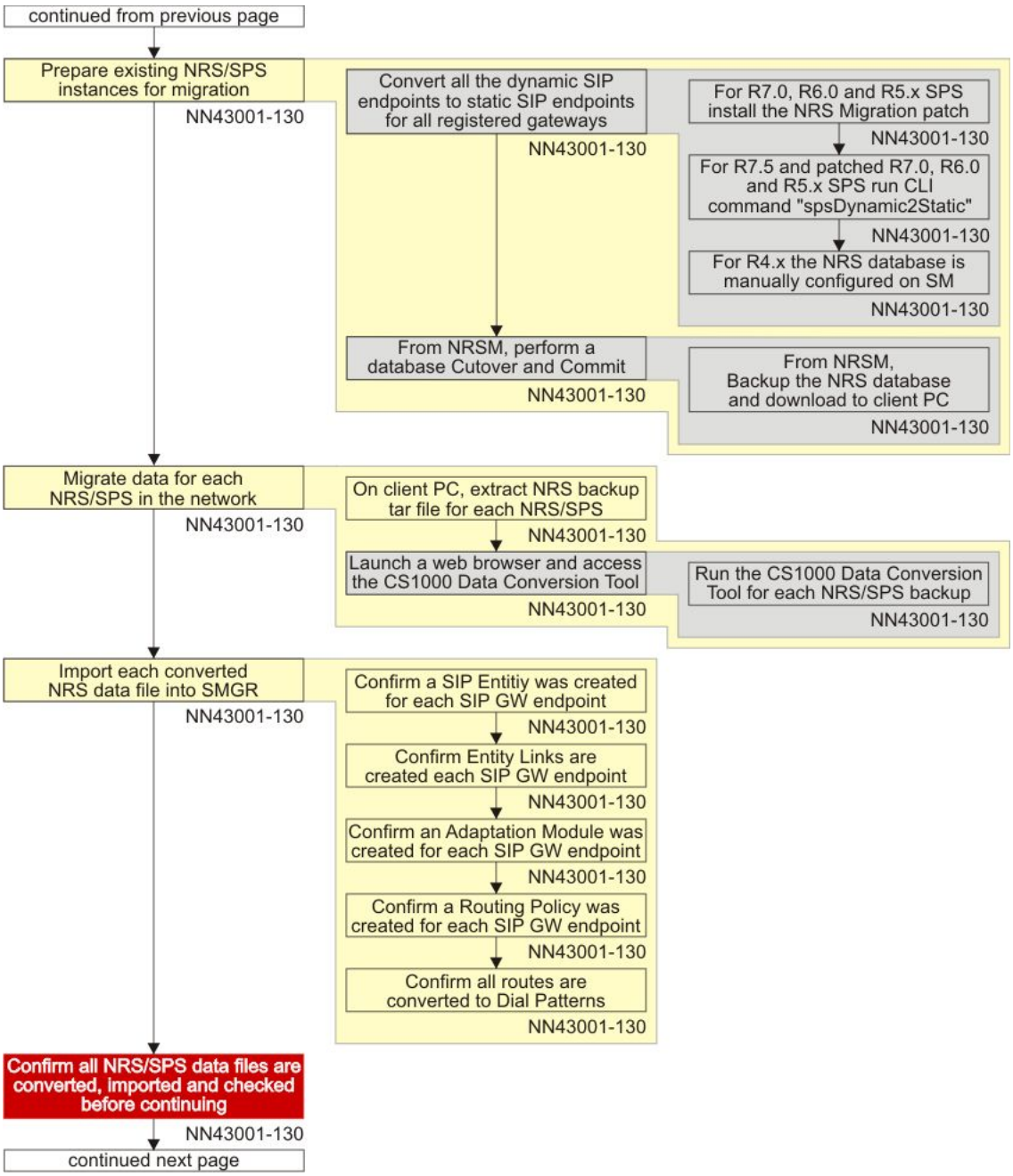
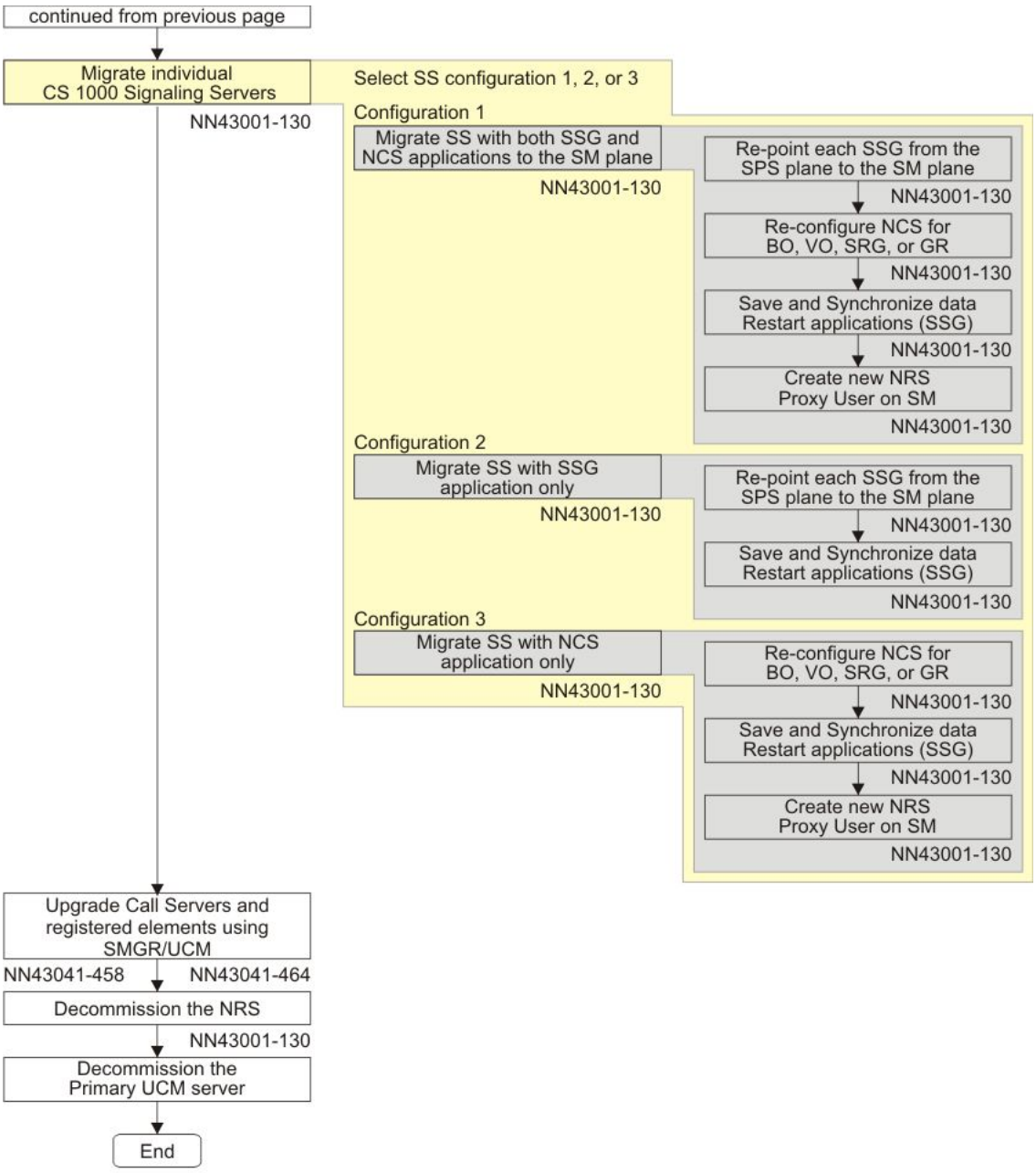


Figure 2: Option One task flow 2

Comments? infodev@avaya.com



Avaya Aura Documentation
Note #1: Installing and Upgrading Avaya Aura™ System Manager
Note #2: Installing and Configuring Avaya Aura™ Session Manager

Figure 3: Option One task flow 3

Option Two task flow

The following four figures provide the CS 1000 Option Two migration to System Manager (SMGR) and Session Manager (SM) task flow.

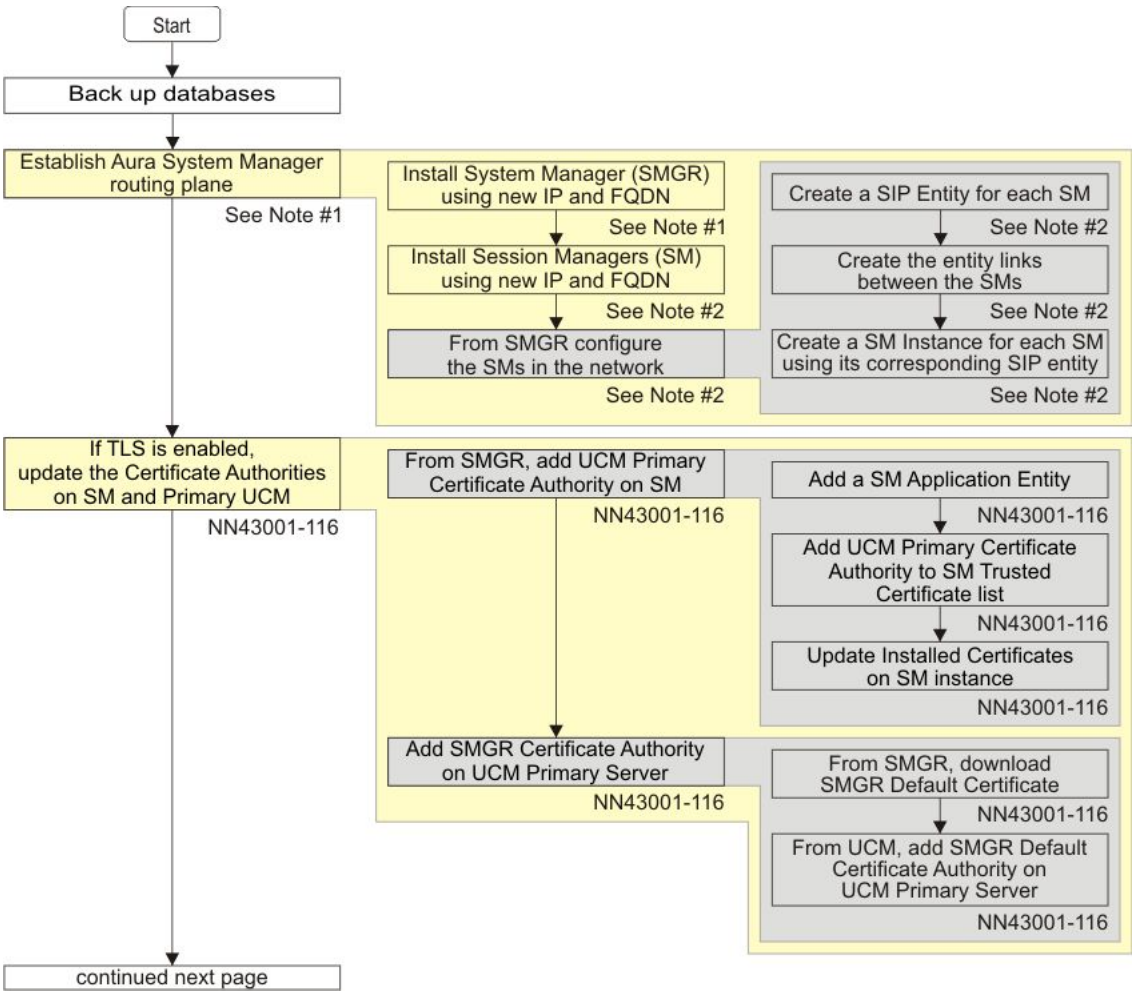


Figure 4: Option Two task flow 1

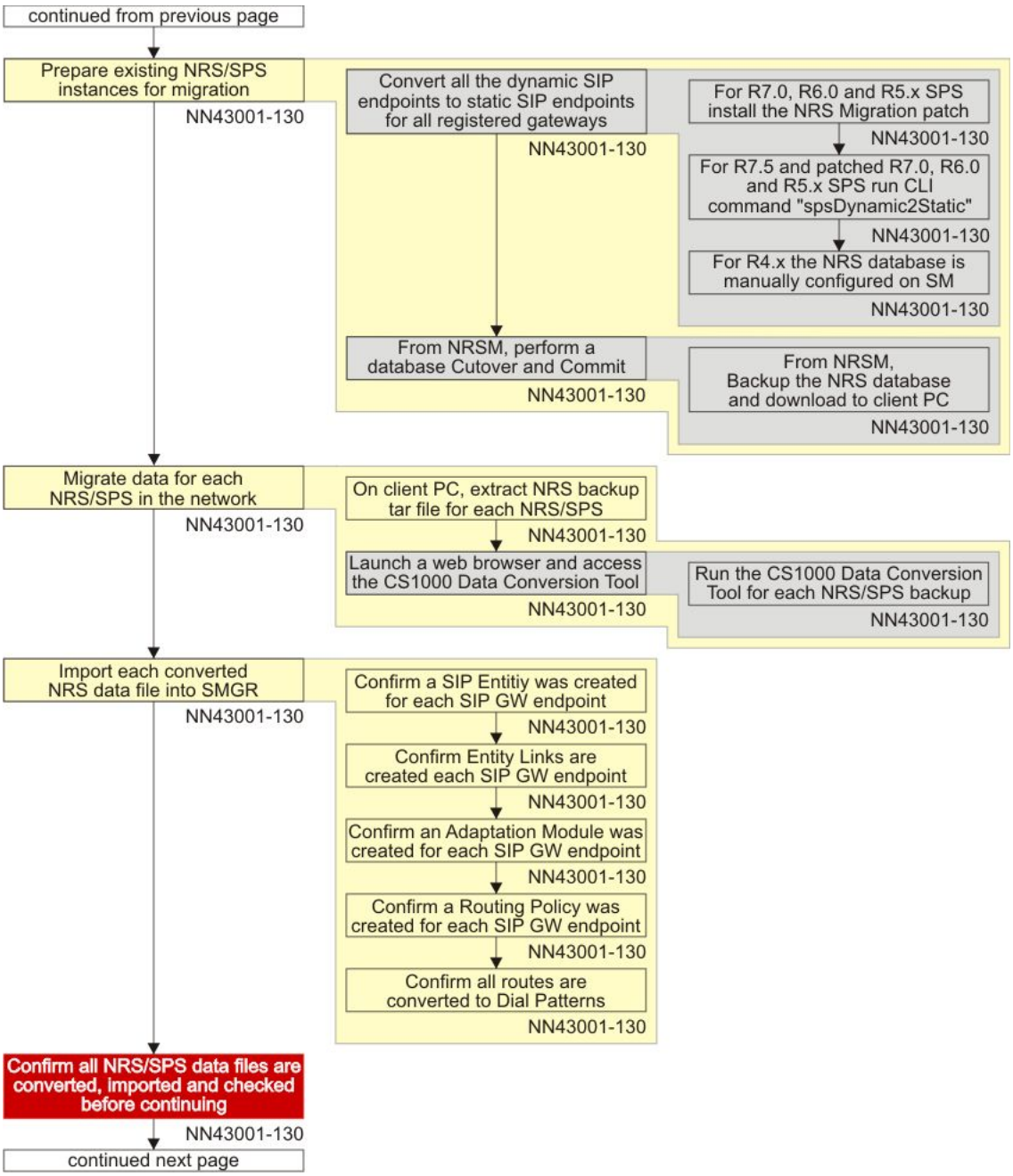


Figure 5: Option Two task flow 2

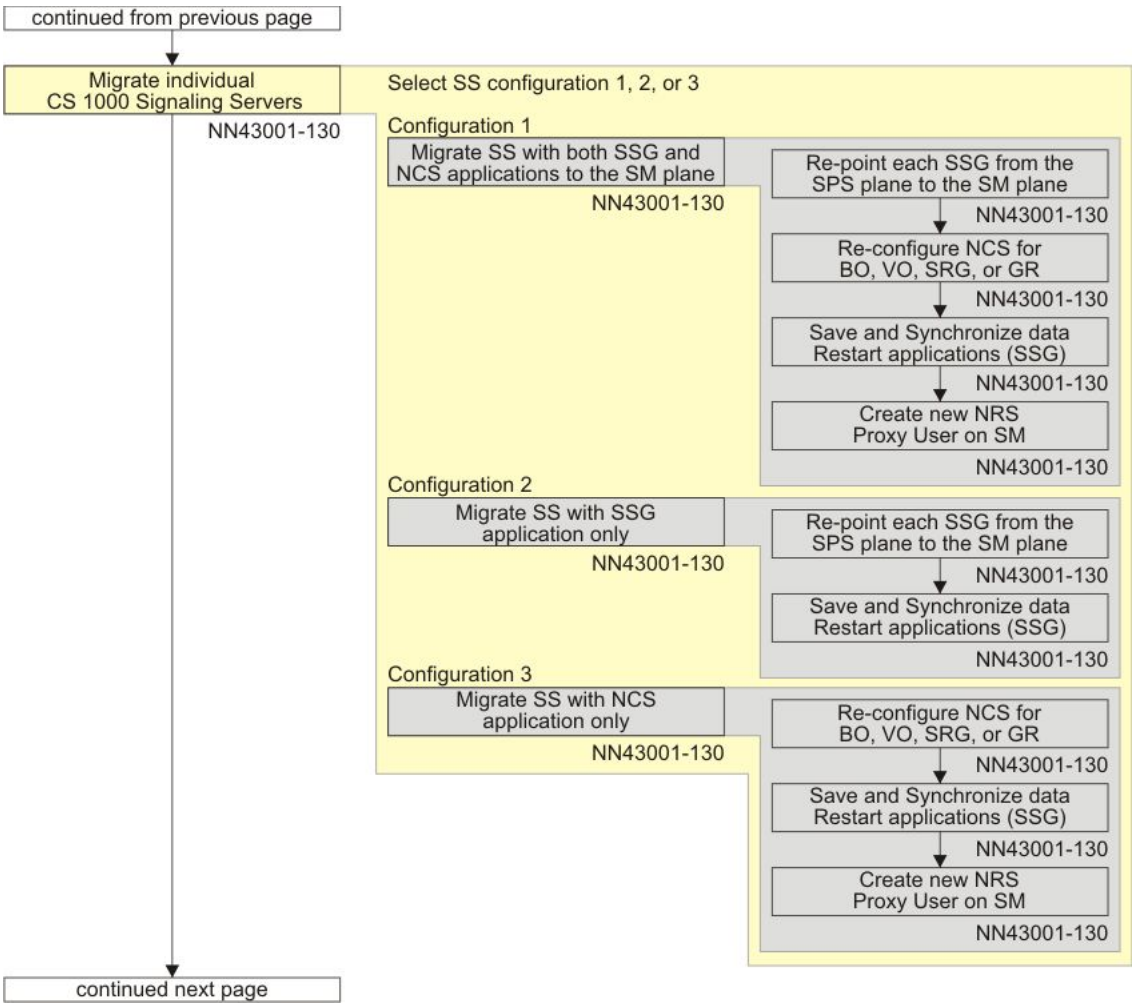


Figure 6: Option Two task flow 3

Comments? infodev@avaya.com

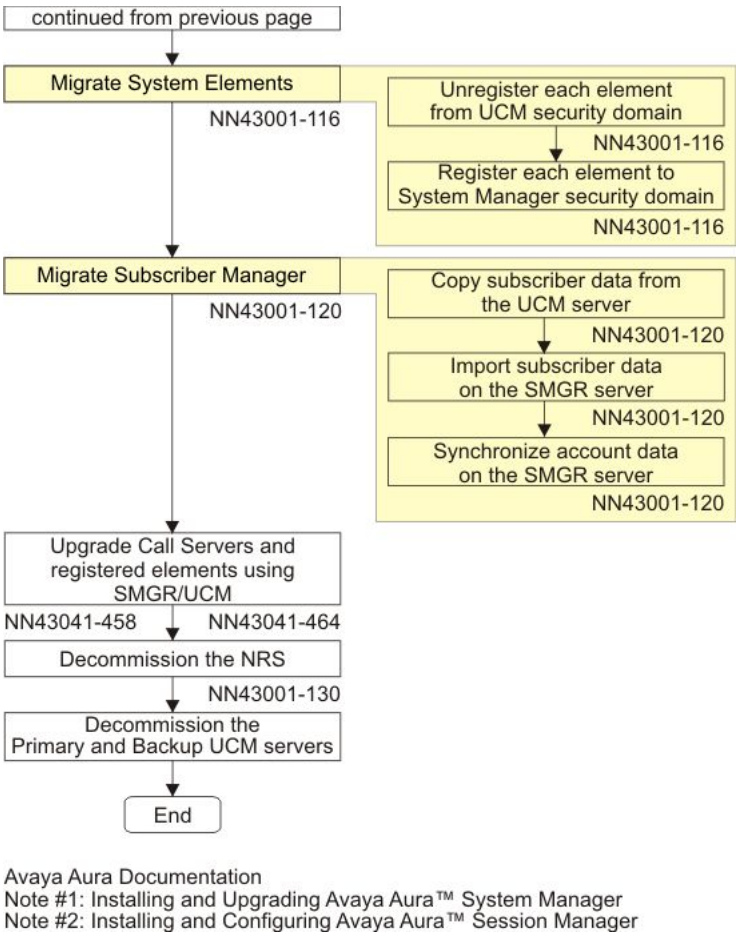


Figure 7: Option Two task flow 4

UCM

You can access a UCM server by using either FQDN or IP address. If you access a UCM server through its FQDN, single sign-on is enabled and you can further navigate from one server to another from the UCM interface without logging in again. If you access a UCM server through its IP address, single sign-on is not enabled. When navigating from one server to another from the UCM interface, the user must log in again to the target server.

Network Routing Service

To support new features, the NRS must be running the latest software release in the network. In most cases, if the entire network is being upgraded, upgrade the NRS first.

It is possible to operate CS 1000 Release 7.5 nodes with CS 1000 Release 5.5 NRS for a short time if the upgrade logistics require this. Some new feature capability may not operate.

Note that the NRS must be the same software release as the Alternate NRS in order to synchronize the databases.

The NRS can operate in two modes: stand-alone or co-resident. Stand-alone and a co--resident NRS are handled differently during a network upgrade. If the NRS is co-resident with a gateway, the entire node must be upgraded.

If you are migrating an existing NRS to Avaya Session Manager, migration requires the replacement of the traditional CS 1000 NRS/SPS and UCM components with new Aura 6.1 Session Manager and System Manager components. All new Communication Server 1000 installations are provided with an Session Manager, and all existing NRS installations 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
- SSMG Tertiary NRS server

NRS installations that do not migrate can continue to use existing NRS functionality.

For more information about migrating NRS to Session Manager, see *Network Routing Service Fundamentals, NN43001–130*.

System and network level security

This section provides an overview of the system and network level security mechanisms. It includes the following:

- Security domain on page 40
- Central and local authentications on page 42
- Intra-System Signaling Security or IPsec on page 42
- Datagram Transport Layer Security on page 44

Security domain

A security domain is a centrally managed collection of elements which includes call servers, signaling servers, media gateways, or media cards that belong to CS 1000 systems, as well as standalone servers. For example, a server running an NRS that operates at the network

Comments? infodev@avaya.com

level. The centralized management functionality is implemented by a primary CS 1000/UCM security server (along with an optional secondary UCM security server).

Note:
Avaya System Manager does not support backup or secondary servers.

For more information about security domain, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Security domain considerations and guidelines

The security domain is established after the primary security server is installed and configured. The following is a high-level list of considerations and guidelines for installing and configuring a security domain:

Considerations and guidelines
Ensure the latest patches are installed on all systems. For information about patching, see *Patching Fundamentals, NN43001–407*.
If you are using DNS, configure DNS first.
Install and configure the primary CS 1000/UCM security servers (and if desired, the backup security servers) before any other elements. Ensure they are fully patched. **Note:** Systems migrated to Avaya Session Manager do not support backup security servers. For information about installing and configuring the primary and backup security servers, see *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.
The FQDN of a UCM security server is associated with its TLAN IP address. You must always configure a security server using the TLAN.
The PC used for web browser access to UCM must be connected to the TLAN (except for networks in the Managed Services configuration). If no DNS server is in use, the PC hosts file should include an entry containing the TLAN IP address and FQDN of the primary security server.
Ensure that all elements can communicate with the UCM security servers. When required, configure static routes.
Register VxWorks-based servers and devices using the ELAN IP address of the UCM primary security server. You require a CLI (telnet, rlogin or ssh) connection for this. For information about registering VxWorks devices, see *Avaya Security Management Fundamentals, NN43001-604*.
Register Linux-based servers and devices using the TLAN FQDN of the UCM primary security server. For information about registering Linux devices, see *Avaya Security Management Fundamentals, NN43001-604*.

Considerations and guidelines
Use the Secure FTP Token Management page to validate successful registration by generating and distributing the token to all elements. For information about generating the Secure FTP Token, as well as information about overall security management, see *Avaya Security Management Fundamentals, NN43001-604*.

Central and local authentications

UCM provides central authentication and authorization for system management and supports access across a security domain. However, the standalone systems uses the local authentication and authorization mechanisms.

The authentication mechanism differs depending upon the servers registering the security domains:

- Call Servers not registered to the security domain -- System management and support users log in to the ADMIN, ADMIN2, PDT1, PDT2 and various LAPW accounts locally. The call server locally authenticates the account login based on the password provided and authorizes the functionality that can be accessed based on the account used.
- Signaling server not registered to the security domain -- Users log in to ADMIN2 accounts, with the signaling server itself being responsible for local authentication and authorization. On the signaling server (only), the ADMIN2 account is still available for login when central authentication is in place, and this specific account continues to be locally authenticated and authorized.
- Call server or signaling server registered to the security domain -- System management and support users log in with accounts defined in UCM. UCM authenticates the user, based on the password provided and authorizes the functionality that can be accessed based on the permissions that the user has been assigned. UCM operates at the security domain level, so users and their permissions are managed centrally, and authentication is performed centrally.

Important:

After registering the security domain, situations can arise where an element is unable to reach either the primary or the secondary UCM security server. Under these emergency circumstances, users with UCM network administrator permissions can log in locally to the element.

Intra-System Signaling Security or IPsec

Intra-System Signaling Security (ISSS) refers to the use of the IPsec protocol to secure traffic within a CS 1000 system. Applications such as Element Manager and Personal Directory or Unicode name Directory uses the ISSS security Servers hosting standalone NRSs and UCMs that operate at the network level do not participate in or make use of ISSS.

Comments? infodev@avaya.com

The pre-shared key for ISSS can be configured by system basis or by security domain basis. One CS 1000 system is used in general and one security domain is used for small networks where it is acceptable for all servers to have the same pre-shared key.

The following table shows the security levels supported for ISSS:

Table 9: ISSS levels definition

ISSS level	Release 5.0 or 5.5	Release 6.0	Comments
Optimal	For known IPsec targets, PBXLink and XMSG are protected by IPsec. For unknown IPsec targets, PBXLink and XMSG are allowed without IPsec.	For known IPsec targets, PBXLink and XMSG require IPsec on ELAN. For unknown IPsec targets, PBXLink and XMSG are denied on ELAN. For both known and unknown IPsec targets, all other protocols are allowed without IPsec.	This secures the PBXLink and XMSG connections and restricts these protocols to known IPsec targets on the ELAN. IPsec is not used to protect any protocols on the TLAN.
Functional	For known IPsec targets, BOOTP, NTP, SSH/SFTP and SSL/TLS are allowed and do not use IPsec. All other protocols on the ELAN require IPsec. For unknown IPsec targets, all protocols are allowed without IPsec.	Not supported	
Full	For known IPsec targets, BOOTP, NTP, SSH/SFTP and SSL/TLS are allowed and do not use IPsec. All other protocols on the ELAN require IPsec. For unknown IPsec targets, BOOTP, NTP, SSH/SFTP, SSL/TLS and AML are allowed and do not use IPsec. All other protocols on the ELAN are denied without IPsec.	For known IPsec targets, BOOTP, NTP, RADIUS, SSH/SFTP, HTTPS and LDAPS are allowed on the ELAN and do not use IPsec. All other protocols on the ELAN require IPsec. For unknown IPsec targets, BOOTP, NTP, SSH/SFTP, HTTPS and LDAPS are allowed and do not use IPsec. All other protocols	ELAN is fully restricted. Only port 443 is allowed without IPsec for HTTPS on ELAN. When you do the configuration to use the different port on the ELAN, IPsec will appear. IPsec is not used to protect any protocols on the TLAN. New elements must register the security domain using manual mode. System mode

ISSS level	Release 5.0 or 5.5	Release 6.0	Comments
		are denied on the ELAN.	register will not be available.

Important:
Before upgrading to CS 1000 Release 7.5, manually disable ISSS on the system where it was previously used.

Datagram Transport Layer Security

Avaya CS 1000 Release 6.0 and later provides signaling encryption for UNIStim IP Deskphones based on the industry standard Datagram Transport Layer Security (DTLS) protocol RFC 4347. Various configuration options of this feature can be combined to form three sets, each with its own level of security. The levels are Basic Security, Advanced Security, and Complete Security.

Important:
The configuration of the security levels must be done sequentially. For example, to configure or upgrade the network to Complete Security, the system administrator has to enable the Basic Security, upgrade the Advanced Security, and finally upgrade the Complete security.

The following table Table 10: Security levels on page 44 describes the security levels in detail:

Table 10: Security levels

Name	Description	Limitations	Level of security	Intended use
Basic Security	Most of the systems on the network are upgraded and configured for DTLS, but there may be systems which do not support DTLS (such as SRG or BCM) or which are not yet upgraded to 7.0. DTLS policy on the 7.0 systems is set to **DTLS Best Effort**	None. This configuration does not pose any limitations on the hardware or software.	Average	This level is suitable for most customers as it provides the signaling security when the hardware or software combinations allow, and does not introduce any limitations.

Comments? infodev@avaya.com

Name	Description	Limitations	Level of security	Intended use
Advanced Security	DTLS is enabled in all the systems in the network and are set to `DTLS Best Effort`	There cannot be any DTLS-incapable systems in the network.	Good	This security level is intended for customers who require more security. But they must use DTLS-incapable phones (such as Polycom conference phone 2033 or Wireless Phones 221x series).
Complete Security	All systems in the network are DTLS-enabled and set to `DTLS only`	There can be no DTLS-incapable equipment on the network, servers, or IP Deskphones. Connecting a phone with an old firmware version may require creating an isolated IP Telephony Node in a black LAN.	Best	This security level is intended for customers who require encryption of every bit of information on the network, such as military or government institutions.

Network Time Protocol configuration

One of the Linux elements of the system (usually the element where Element Manager runs) is designated as the system primary Network Time Protocol (NTP) server. Another element may optionally be designated as a system secondary NTP server. These system primary or secondary NTP servers usually synchronizes to external NTP clock sources, but can also utilize their internal hardware clocks. The secondary NTP server would only be used if the primary NTP server is unavailable.

Other Linux system elements synchronize time from these two servers using NTP. If the Call Server is on VxWorks it synchronizes with these system primary and secondary NTPservers. Other VxWorks devices, such as Gateway Controllers, continue to get time updates directly from the Call Server.

When upgrading a CS 1000 system configure NTP settings using Element Manager (EM). Previous settings on the Call Server, such as external NTP clock sources, are extracted and

presented as defaults. NTP configuration performed by EM is applied to all system elements. If this EM configuration of NTP is not performed, then NTP will not function correctly for the system.

For information about NTP configuration, see *Element Manager System Reference - Administration* (NN43001-632).

Other Linux elements that are not part of a CS 1000 system (for example, standalone NRS, standalone UCM primary security server) must be configured individually for NTP synchronization. These would normally point to external NTP clock sources. The UCM Base Manager of each element should be used for NTP configuration.

Deployment considerations

This section describes deployment options to consider for supported configurations:

- Management of IP telephony nodes on page 46
- Personal directory and unicode name directory on page 47
- Primary and secondary NRSs on page 47
- Element manager on page 47
- Primary and secondary UCM security servers on page 48
- Subscriber Manager on page 49
- Survivable Remote Gateway on page 49

Management of IP telephony nodes

SIP line, UNIStim line TPS (LTPS), and virtual trunk (VTRK) applications running on the signaling servers in an IP telephony node are managed as a group. The Leader Signaling Server and Follower Signaling Servers in a node are linked to a single call server, and an election is run to select a Follower Signaling Server to act as the leader and takes on the node IP address when the Leader is not available. There is only one set of configuration settings (node ID, call server IP address, TLAN node IP address and subnet mask, ELAN gateway IP address and subnet mask) per node.

Node management features cluster manager, where a cluster represents a group of physical servers which shares the same configuration properties. The same set of services are configured and enabled on all physical servers within a Cluster.

Element Manager is used to configure application services. There is no server level configuration for application services and they are applied at a Nodal level where all servers that belong to the Node share the same set of services.

The Node must have minimum one server as a Node element in order for that Node to be operational. The administrator can add as many servers to be part of the Node and all the Node elements will have the same set of application services enabled, however only one physical server can be active at a time. This active server can run all the configured services

on that physical server. For example, UNIStim LTPS and SIP can all be configured and enabled on the same server. The LTPS application is an exception where several servers can run active instances of LTPS service. The LTPS application supports load sharing.

Personal directory and unicode name directory

There will be one instance of the personal directory (PD) application for each system.

The unicode name directory feature (UND) enables the representation of calling or called party name in Unicode and the use of languages other than English for name display. It is provided as part of the PD and is not considered as a separate application. UND requires the Subscriber Manager (SubM) to manage users names in multiple languages.

Primary and secondary NRSs

Ensure that the secondary NRS can provide sufficient capacity to handle the load of the primary NRS in the event of primary NRS failure. To properly support active-active operation, deploy the secondary NRS on an identical hardware platform as the server on which primary NRS is deployed.

Ensure that the combined processing load of all the software packages running on the secondary server is approximately equal to the combined processing load on the primary server. For example, Avaya does not recommend a configuration in which the primary NRS is standalone and the secondary NRS is on a server that runs other signaling server applications. In that case, the secondary NRS would potentially be unable to handle the processing load of the primary NRS.

Important:

Configuration of nodes can be modified only from the primary NRS. When both the Primary and Secondary nodes are in service, the database on the Secondary server is read-only. An administrator cannot change configuration information on the Secondary Server except when the Primary Server is not in service and the Secondary Server cannot connect with the Primary server. Changes on the Secondary Server are overwritten when the Primary Server comes into service.

Element manager

There is one Element Manager (EM) for each CS 1000 system. The Release 5.0 or 5.5 configuration of a server hosting multiple EMs to serve multiple CS 1000 systems is no longer supported. In general, TDM systems can be managed by command line without requiring EM (which needs to run on a Linux-based signaling server).

Primary and secondary UCM security servers

The primary UCM security server provides:

- centralized authentication and access control for all of the servers in the domain.
- a registration repository for all of the servers.
- central launch point for the element managers of each system in its security domain.
- security functions such as issuing of X.509 certificates, configuration of the IPsec pre-shared key, and configuration of the security token used in application-level file transfer between servers.
- service as the consolidation point for the OA&M logs from all of the servers, if OA&M log consolidation is enabled.

The combination of these functions implies that the availability of the primary UCM security server directly impacts the management and support operation of the systems in the security domain, and could indirectly impact runtime activities as well in some cases.

Note:

On migrated systems the System Manager/UCM does not use secondary servers.

The secondary CS 1000/UCM security server provides a subset of the functionality of the primary, including centralized authentication, and access control. When primary server is down, there is no automatic procedure to recombine the logs consolidated on the secondary with the logs previously consolidated on the primary after the primary comes back up.

To ensure that the secondary UCM security server can provide sufficient capacity to handle the on-going processing load of the primary in the event that the primary fails, the secondary needs to be deployed on an identical hardware platform (that is, same type and vendor) as the server on which the primary is deployed. In addition, the combined processing load of all of the software packages running on the secondary server should be approximately equal to the combined processing load on the primary server.

It is not recommended to have a Co-resident Call Server and Signaling Server system as the primary or secondary UCM security server for more than one system. This is to minimize the impact of management processing load on the call processing that needs to take place on the co-resident server within its CPU and memory envelope.

Important:

If a signaling server is running applications such as LTPS, VTRK, and SLG, it may be considered expendable. However, a signaling server hosting a primary or secondary UCM security server has a much greater requirement to be up continuously Also, in campus and geographical redundancy scenarios, the placement of the primary and secondary UCM security servers should minimize the likelihood that a temporary or long-term (For example, due to disaster) unavailability of a system or site disrupts the operation of the entire security domain.

Comments? infodev@avaya.com

Subscriber Manager

Subscriber Manager (SubM) is deployed as a plug-in application above UCM Common Services. SubM provides a central location to manage subscriber information for enterprise services. With SubM, users can easily manage subscribers and subscriber accounts (phone services) within a network. The SubM runs only on the UCM primary security server, that is, there is only one instance of SubM per security domain.

For more information about SubM and how to configure subscribers and subscriber accounts (phone services), see *Subscriber Manager Fundamentals* (NN43001-120).

Survivable Remote Gateway

Enable FTP to interoperate with existing releases of the Survivable Remote Gateway (SRG). If using SRG Release 3.0 or earlier, you must enable FTP on all Linux boxes running signaling server UNIStim DTLS applications.

Comments? infodev@avaya.com

Chapter 6: Upgrading the IP telephony network

This section provides a high-level task flow for the installation or upgrade of an Avaya Communication Server 1000 (Avaya CS 1000) system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the publication number that contains the detailed procedures required for the task.

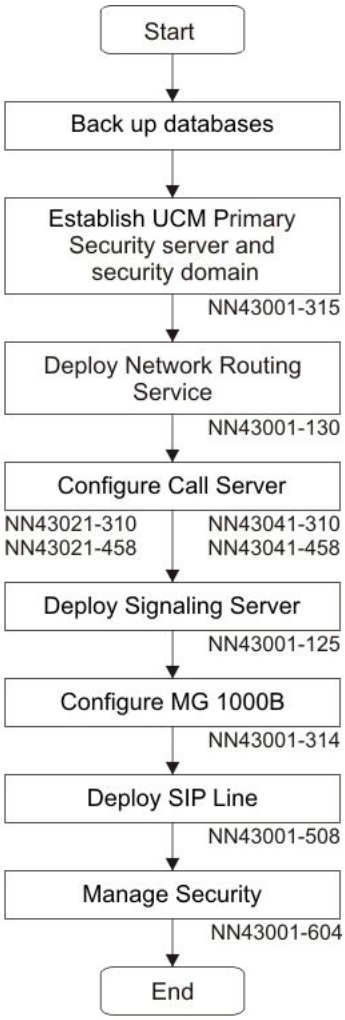


Figure 8: Steps for central upgrade

When planning a network-wide upgrade, first migrate the components that are network-wide resources, then update the individual nodes.

Turn on the FTP before the upgrade on both the call server and the signaling server. You can turn off the FTP after the upgrade is complete to improve the security. FTP is turned on for each subsequent Gateway Controller or media card that is added or repaired.

For information on how to change the FTP settings using CLI see Avaya *Communication Server 1000 Security Management Fundamentals* (NN43001-604).

Full deplist through the Software Media is not delivered as the user need to download the current patches recommended in realtime. The prompt to install a DepList applies only if there is one being delivered during the software installation. This is done to avoid the conflict between the patches during upgrades.

UCM

You can upgrade Unified Communication Manager (UCM) using two upgrade paths:

- Complete upgrade to UCM
- Gradual upgrade to UCM from ECM

Complete upgrade to UCM

A single network UCM upgrade from Release 5.x, or 6.0, or 7.0 must be carried out in a single maintenance window. Enter `upgrade` command from a 5.x Primary server's command line interface (CLI) to perform the upgrade. To upgrade the single system use the following steps:

Upgrading the Linux server

1. Login to the linux server as a user within the system admin group.

   In Release 6.0 or higher any user having system admin group privileges can perform upgrade.

2. Type `upgrade` on the CLI.
3. Optionally, you can save the backup data. To save the backup data in an external source such as the USB device or an SFTP server enter `Y` for the question shown in the following prompt and enter information requested regarding the external source.

```
System data will be saved at /admin partition.
Please use option "Re-use /admin partition" during Linux Base
installation.
Do you want to backup data to external source (USB/SFTP) as well?
(Y/N) [Y]?
Backup started. Please wait...
INFO - Initializing ThreadPoolExecutor
INFO - Result=Quantum backup restore completed Successfully.
Status=Quantum back up restore completed.
Backup complete.
```


Comments? infodev@avaya.com

```
Please insert Linux Base Media for upgrade, then press ENTER key
(a reboot will occur)
```

4. Insert the media with the linux base software in the drive (DVD for COTS servers and CF for CP PM servers) and press the `Enter` key.

Important:

Do not enter n in the following prompt else the admin partition will get formatted.

```
Existing Configuration Partition Usage

--------------------------------

A pre-existing administration partition has been found on
this system.

If this re-installation is due to a possible disk
corruption, it is recommended that you format this
partition to avoid any file corruption that may be present.
In this case, all data will be removed from this partition
and you will be required to manually enter all installation
questions from the beginning.

If this re-installation is not due to disk corruption, then
leaving the partition is a safe option, and if valid data
from the previous configuration exists, you will be given
the option of reusing that data during this installation.

Do you wish to format the administration partition (Y/N)
[N]? n
```

5. Choose option 1 in the following screen to reuse the existing information.

```
Configuration Data Selection
----------------------------
A pre-existing system configuration data file has been found on
this computer.
You may choose to do one of the following:
1) Reuse the data from this pre-existing configuration file. The
data input-validation-screens will be shown for validation.
2) Use backed up data from a USB device. (Note: only one USB
device should be plugged-in when prompted.)
3) Use remote backed up data from a SFTP-server. This requires
the      provision of SFTP server information.
4) Ignore the data in pre-existing configuration file.
The standard system-configuration-prompts will be presented.
Select an option (1-4):

1
```

6. To restore the base application, enter `Y` in the following prompt:

```
Base data recovery
------------------
```

```
Base data includes the following settings:
- system hardening setting
- Jboss-Quantum application setting
- oam-logging application setting
- Snmp-Daemon-TrapLib application setting
Do you want to recover Base data? (Y/N) [Y]?

y
```

When you have upgraded the linux base, you will need to upload the software to the deployment server. Use the following steps to upload the software:

Uploading software to the deployment server

1. Login to primary UCM using the admin account, when the linux base is upgraded

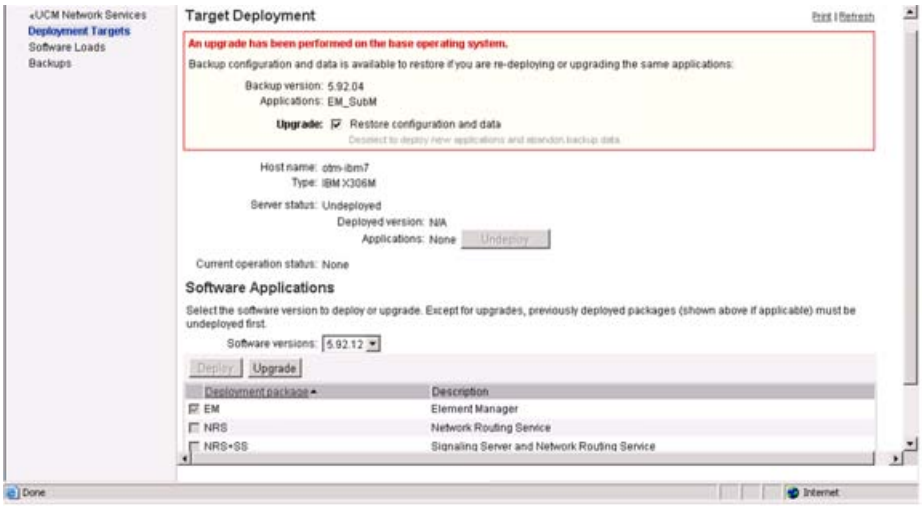
   Important:

   You need to login to the primary even if you have upgraded a member server.
2. Click on the **software deployment** link.
3. Click on the **software loads** link in deployment manager (DM) to upload the application software.
4. In DM, from the targets page, select the server's radio button.
5. Click **Deploy**.

   Target deployment screen gives an option for upgrade and displays the previous deployment in an upgrade box on top of the screen.
6. **Important:**

   The packages are pre-selected as the previous deployment, and the **Upgrade** button is enabled.

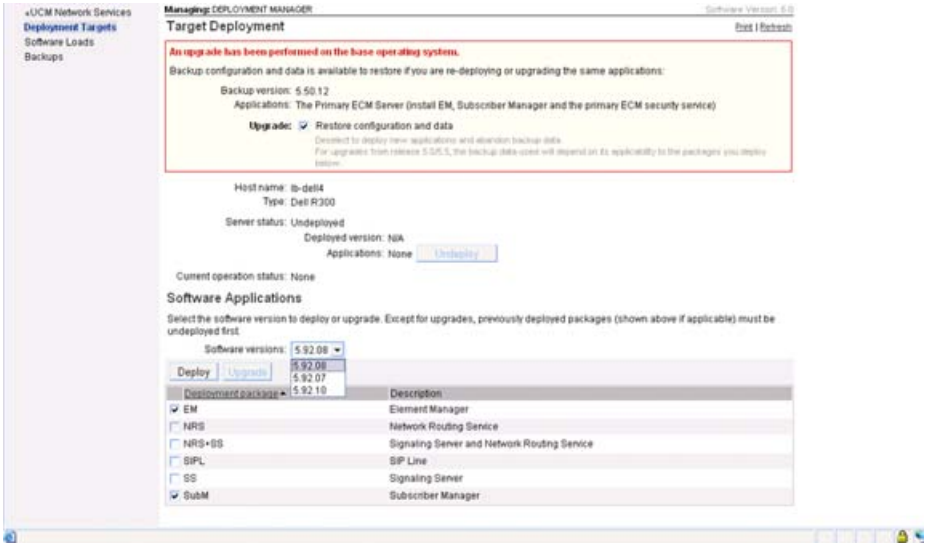
   Choose the software version to upgrade to and click **Upgrade**.



Comments? infodev@avaya.com

7. **Important:**

   If you are upgrading a Release 5.0 or 5.5 system, the **Deploy** button is enabled.



   Choose the software version to upgrade to.

8. Choose the packages to be deployed and click **Deploy**.

   When the deployment is completed, the server is ready for operation.

Upon a successful upgrade, the manual security configuration is not required and the server is installed as a 7.5 Primary UCM Security server. The data from the 5.x server is restored.

Following are the details of data restore:

- Certificates -- None of the certificates and list of trusted certificate authentications (CAs) from the 5.x server are restored. The private key from the 5.x server's private CA are reused to create a new private CA for the 7.5 server.
- Roles -- All built-in and user defined roles are migrated. The permission mappings are lost. The permissions have to be mapped manually to the roles.
- Users -- All internal and external users are restored. The users will have the same role mapping as before. The default role for the user admin is Network administrator. In the 5.x database all user account passwords are hash encrypted.
- Elements -- UCM 6.0 and later does not support Release 5.0 and 5.5 CS 1000 application versions of EM, BCC, NRSM, and Subscriber Manager applications. Hence, none of the CS 1000 Release 6.0, NRSM, SIP Gateway, and Subscriber Manager type elements are restored. The Element type for each element is converted to a Hyperlink.
- Policies -- User account and password policies are not restored. New accounts are created in keeping with the default values of the new release. Information and configuration of External Authentication servers are not restored.

Gradual upgrade to UCM from ECM

A mixed network is a network that contains CS 1000 Release 7.5 systems, and systems that are still running Release 6.0 or 5.5, and has been using ECM. In mixed networks, both ECM and UCM are required. You must perform a mixed network UCM server upgrade when the entire 5.x ECM security domain cannot be upgraded to CS 1000 Release 7.5 at once. Networks running both CS 1000 Release 6.0 and CS 1000 Release 7.5 must maintain two primary UCM servers. When all the systems are upgraded to Release 7.5 you can remove the Release 5.x or 6.0 primary COTS server from service and reuse it elsewhere.

The prerequisites for this upgrade are a fully configured 5.x Primary ECM server and a backup file from it.

Follow these steps to perform a mixed network upgrade:

1. Type `admin2` as the username to log in to the CLI of the 5.x ECM Primary server.
2. Enter the command `sysbackup -b` to generate a backup archive.
3. Install a CS 1000 Release 7.5 UCM server.

   Ensure that the CS 1000 Release 7.5 UCM server is freshly installed without any reference to an existing backup file or configuration file.
4. Type `admin2` as the username to log in to the UCM 6.0 server CLI.
5. Enter `sysrestore` command and select the backup file generated from the ECM 5.x server in step 1 on page 56.

   The server is configured as a CS 1000 Release 7.5 Primary UCM security server. Only UCM specific data is restored from step 2 on page 56.

The Primary UCM server has a RADIUS authentication server running on it. In order to synchronize user accounts, the Primary UCM server must act as the RADIUS server and the 5.x Primary ECM server as the RADIUS client. Configure an External RADIUSAuthentication server on the Release 5.x Primary ECM server. For more information about configuration details, see *Enterprise Common Manager Fundamentals* (NN43001-116). The following details are required to setup RADIUS authentication on the Release 5.x Primary ECM server:

`RADIUS server IP ->` IP of the Release 6.0 UCM Primary server.

`RADIUS shared secret ->` Login to the CLI of the Release 6.0 Primary UCM server as “admin2” user and execute the following command to retrieve the shared secret.

`RADIUS port ->` 1812 can be used by default.

If the Release 5.x Primary ECM server already has an external RADIUS server configured, that server should be configured as the external RADIUS authentication server for the Release 6.0 Primary UCM server.

Following are the details of data restore:

- Certificates -- You can transfer the information required to bridge the trust between CS 1000 Release 5.x systems and Release 6.0 systems by restoring the Release 5.x Primary backup data into the UCM 6.0 primary. The private key from the Release 5.x server private

Comments? infodev@avaya.com

CA is reused to create a new intermediate private CA for the CS 1000 Release 6.0 server. As a result, certificate details remains the same. The certificate start date refers to the current date, and the certificate friendly name and common name refer to the CS 1000 Release 6.0 server FQDN.

- Roles -- All built-in and user defined roles are migrated. The permission mappings are lost. The permissions have to be mapped manually to the roles.
- Users -- All internal and external users are restored. The users have the same role mapping as before. The default role for the user admin is Network administrator. In the Release 5.x database all user account passwords are hash encrypted.
- Elements -- The Release 6.0 UCM server acts as a launch point for all Release 5.x elements. All the Release 5.x elements are migrated to Release 6.0. The Element type for each element is converted to a Release 6.0 Hyperlink.You can not perform certificate related operations on the migrated elements.
- Policies -- No user account and password policies are restored. They are set as per the defaults mentioned in Release 6.0. Information and configuration of External Authentication servers are not restored either.

Following are the limitations in a mixed network:

- Single sign On -- System partially supports the Single Sign On between the Release 6.0 UCM network and the Release 5.x ECM network. Users are prompted for a user name and password only for the first time to launch a 5.x management application of a 5.x element. Thereafter the SSO cookie automatically authenticates any subsequent login, provided the user does not logout from the managed application or the session does not expire or terminate.
- Elements 5.x -- 5.x Elements cannot be added from the 7.5 Primary UCM server and vice-versa. Results of Edit and Delete operation carried out on a primary server will not reflect on the other. The changes made on the 5.x primary server decides the behavior of the Release 6.0 or 5.5 managed elements and changes made on the Release 7.5 primary server will decide the behavior of the CS 1000 Release 7.5 managed elements. The 7.5 UCM network acts as a unified launch point for all managed elements an administrator is concerned with.
- Users -- The roles mapped to the same user in 5.x server can be different from the mappings in the Release 6.0 server, because some roles are no longer valid in CS 1000 Release 6.0. This causes functional differences in Release 5.x and 6.0 environments.

NRS or SPS

In order to support new features, the Network Redirect Server (NRS) or SIP Proxy Server (SPS) must be running the latest software release. In most cases, if the entire network is being upgraded, upgrade the NRS first.

The Linux NRS has redirect server functionality, so it can operate in either redirect or proxy mode on a per-endpoint basis.

It is possible to operate CS 1000 nodes with CS 1000 Release 5.5 if the upgrade logistics require this.

The Linux SPS is part of the Linux NRS. For security certificates porting, it is part of UCM enhancement. The certificate is under UCM control. SIPGW and Linux NRS make use of this. You can export the certificate in the 5.5 or earlier Release and import them back into the CS 1000 Release 7.5.

Important:

The NRS must normally be the same software release as the Alternate NRS in order to synchronize the databases.

The NRS can operate in two modes: stand-alone or co-located. A stand-alone and a co-located NRS are handled differently during a network upgrade. If the NRS is co-located, the entire node must be upgraded.

Upgrading with a stand-alone NRS

1. Separate the NRS nodes so that they do not automatically synchronize.
2. Separate any Failsafe NRS.
3. Upgrade the Primary NRS.
4. Upgrade the Alternate NRS.
5. Re-synchronize the Primary and Alternate NRS.

Upgrading with a co-located NRS

1. Separate the NRS nodes so that they do not automatically synchronize.
2. Separate any Failsafe NRS.
3. Upgrade the entire node.
4. Re-synchronize the Primary and Alternate NRS when both are running the same new software releases.

For more information about NRS upgrade procedure, see *Network Routing Service Installation and Commissioning* (NN43001-564).

Survivable Remote Gateway

Survivable Remote Gateway (SRG) upgrades the IP Deskphone and redirects the IP Deskphone back to the CS 1000 system. To interoperate with existing releases of the SRG, enable the FTP protocol on the CS 1000 system. As the FTP protocol is generally considered to be insecure, there is a tradeoff between the use of SRG and the amount of security provided by the system.

Comments? infodev@avaya.com

CS 1000M

For more information about CS 1000M upgrade see, *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458).

CS 1000E

To convert CS 1000E CP PM VxWorks based systems to the Linux based CS 1000E CS and Signaling Server Co-resident CP PM platform perform the conversion in the following order:

1. Upgrade Hardware (RAM and hard drive)
2. Upgrade BIOS and CP PM latest version
3. Install Linux base software
4. Install CS 1000 Release 7.5 and signaling server

For information about BIOS and CP PM upgrade and Linux base installation see *Linux Base Installation and Commissioning* (NN43001-315).

For information on CS 1000 Release 7.5 and signaling server installation, see *Co-resident Call Server and Signaling Server Fundamentals* (NveN43001-509).

CS 1000E TDM only configuration is supported only on the CPPM Co-Res platform. Upgrade for an Option 11C type of system must be done in the following order:

1. Back up the Option 11C database onto Compact Flash.
2. Install the CP PM Co-Res system.
3. Install the backed up Option 11C database.
4. Install and configure the required MGCs for the expansion cabinets.

Avaya MG 1000E

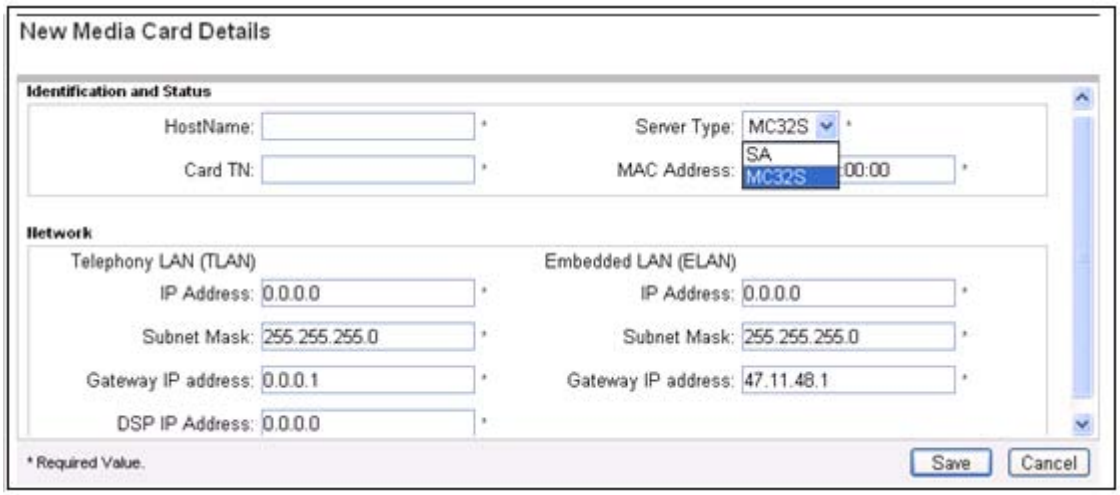
For information about upgrading Avaya MG 1000E, see *Communication Server 1000E Upgrade Hardware Upgrade Procedures* (NN43041-464).

Media cards

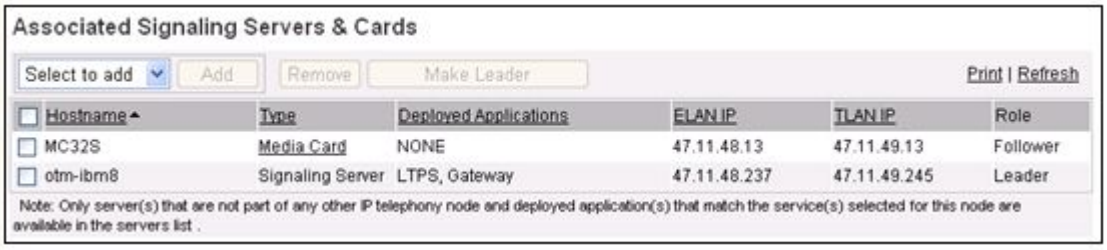
Follow these steps to install the media card:

1. Select the media card from the drop-down list.

2. Enter the following attributes:
   - Hostname
   - Card TN
   - Server Type
   - MAC address
   - ELAN and TLAN IP
   - ELAN and TLAN Subnet Mask
   - Card type
   - DSP IP address



3. Click **Save** to return to Node edit page.
4. Save and Transfer the Node with the Media card configuration.



5. Reboot the Media card for the configuration to take effect.

Signaling Server

For information about the the upgrading the Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Avaya MG 1000B

For information about upgrading the MG 1000B, see *Branch Office Installation and Commissioning* (NN43001-314).

Security settings

For information about how to upgrade security settings, see *Security Management Fundamentals* (NN43001-604).

Setting loadware

For information about setting loadware, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Comments? infodev@avaya.com

Index

A

Add 14
BO 14
Avaya MG 1000B 61
Avaya MG 1000E 59

B

Branch office 14
add 14
Branch Office 16
requirements 16

C

Compatibility matrix 21
Complete upgrade to UCM 52
Configuration 14
Mixed-software 14
CS 1000E 59
CS 1000M 59

D

Datagram Transport Layer Security 44
Deployment considerations 46–49
Element manager 47
Management of IP telephony nodes 46
Personal directory and unicode name directory 47
Primary and Secondary NRSs 47
Primary and Secondary UCM Security Servers 48
Subscriber Manager 49
Survivable Remote Gateway 49
Deployment server upload 52

G

Geographic redundancy 20
operation 20
Gradual upgrade to UCM from ECM 56

M

Main office and Branch Office 17
Main office requirements 15
Media cards 59
Mixed-software configuration 14

N

NRS or SPS 57
NTP configuration 45

O

Optional features 16

P

Primary and Secondary NRSs 47

S

Security levels 44
Advanced Security 44
Basic Security 44
Complete Security 44
Security settings 61
Setting loadware 61
Signaling server 61
Software requirements 13
Main office and Branch Office different release 13
Main office and Branch Office same release 13
Subscriber Manager 49
Survivable Remote Gateway (SRG) 58
System and network level security 40
System and Network Level Security 40, 42
Central and local authentications 42
Intra-System Signaling Security or IPsec 42
Security domain 40

U

UCM 52
Upgrade 52, 56
Complete upgrade 52
Gradual upgrade 56
Upgrade network 52, 57–59, 61
Avaya MG 1000B 61

Avaya MG 1000E 59
CS 1000E 59
CS 1000M 59
Media cards 59
NRS or SPS 57
Security settings 61
Setting loadware 61
Signaling server 61
Survivable Remote Gateway (SRG) 58
UCM 52
Upgrading the IP Telephony network 51