Nortel Communication Server 1000
New in this Release

7.0
NN43001-115, 04.05

August 2010

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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(s) 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 this product. 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://www.avaya.com/support. Please note that if you acquired the product 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, AND 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(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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://www.avaya.com/support/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 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://www.avaya.com/support/. 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(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

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://www.avaya.com/support

Contents

Chapter 1: How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the telephone number for your region:

http://www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Chapter 2: Introduction

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

Subject

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server (CS) 1000 Release 7.0 software. For more information on legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page:

http://www.avaya.com

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)
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

Conventions

Terminology

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

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

Revision history

August 2010	Standard 04.05. This NTP is up-issued to address CRs.
July 2010	Standard 04.04. This NTP is up-issued to address CRs.
June 2010	Standard 04.03. This NTP is up-issued to correct some task flows.
June 2010	Standard 04.02. This NTP is up-issued to include NTP reference updates in the IP Media Services chapter.
June 2010	Standard 04.01. This NTP is issued to support Communication Server 1000 Release 7.0.

Chapter 3: Overview

Communication Server (CS) 1000 Release 7.0 is the latest release for the CS 1000 family of products. CS 1000 Release 7.0 is a further evolution of the traditional TDM enterprise network to a converged IP based network.

The CS 1000 Release 7.0 is a reliable and secure platform for Voice over IP (VoIP) communications and is designed to be a more open and simplified platform, which speeds deployment and improves manageability.

Key Attributes

- Adaptable to meet current and future needs

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

- Superior IP Telephony experience

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

- Improved reliability and security

  Business continuity improvement from a reliable and secure environment

- Simplified convergence solution

  Product portfolio simplified for easier deployment, configuration and management

New for CS 1000 Release 7.0

The following chapters provide a description of what's new in CS 1000 Release 7.0:

- High Scalability system on page 35
- IP Media Services on page 43
- SIP Trunk Bridge on page 45
- New hardware on page 47
- Deployment Manager enhancements on page 51

Packages

CS 1000 Release 7.0 introduces the following new packages:

- High Scalability package 421
- IP Media Services 422

Hardware

CS 1000 Release 7.0 introduces the following new hardware:

- Common Processor Media Gateway (CP MG) card
  - CP MG card with 32 DSP ports (CP MG 32)
  - CP MG card with 128 DSP ports (CP MG 128)
- Common Processor Dual Core (CP DC) card
- 128 port DSP daughterboard (DB-128)

Co-resident Call Server and Signaling Server hardware platforms

CS 1000 Release 7.0 Co-resident Call Server and Signaling Server (Co-res CS and SS) can run the Call Server software, Signaling Server software, and System Management software on a single hardware platform running the Linux Base Operating System.

For CS 1000 Release 7.0, various hardware platforms can support the Co-res CS and SS configuration. The CS 1000E Co-res CS and SS configuration is supported on the following hardware platforms:

- Common Processor Pentium Mobile (CP PM)
- Common Processor Dual Core (CP DC)
- Common Processor Media Gateway 32
- Common Processor Media Gateway 128
- IBM x3350 Commercial off-the-shelf (COTS) server
- DELL R300 COTS server

The IBM x3350 and Dell R300 COTS servers are generically referred to as COTS2 servers, and can support the Co-res CS and SS configuration. The IBM x306m and HP DL320 G4 COTS servers are generically referred to as COTS1, and do not support the Co-res CS and SS configuration.

Note:

COTS2 servers require an NTRH9220E5 USB security dongle adapter, which is provided with the software kit. For increased security, ensure the USB security dongle adapter is hidden from plain view. Do not insert the USB security dongle adapter into a front USB port. Nortel recommends you insert the USB security dongle adapter into the internal USB port on the Dell R300 server, and into a rear USB port on the IBM x3350 server.

For the security dongle to be recognized on COTS2 servers, you must insert the USB security dongle adapter with security dongle into a USB port before you boot the COTS2 server.

Table 1: Co-res CS and SS system types

Server hardware for Co-res Call Server	Signaling Server system types for VxELL Servers
CP PM	4121
CP DC	4221
CP MG	4321
CP MG	4421
COTS2	4521

OAM simplification

CS 1000 Release 7.0 simplifies management by consolidating OAM functionality into the Unified Communication Management (UCM) environment. You no longer need to install and maintain Telephony Manager as part of your CS 1000 infrastructure.

The following Telephony Manager functionality is now available in UCM-based applications (for example, Element Manager, Subscriber Manager):

- Station Management
- Corporate Directory
- List Manager
- Traffic Analysis
- critical ESN configuration functionality
- maintenance windows

For more information about TM functionality available in UCM applications, see *System Management Reference, NN43001-600*.

Documents

CS 1000 Release 7.0 introduces the following new documents:

- *SIP Trunk Bridge Fundamentals , NN43001-143*
- *Communication Server 1000E Planning and Engineering – High Scalability Solutions (NN43041-221)*

- *Communication Server 1000E High Scalability Installation and Commissioning , NN43041-312*
- *Using the DMC DECT Manager , NN43001-142*

Task flows

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

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

This section provides information on the following topics:

Figure 1: Example task flow on page 18 shows an example and how to interpret the task flows.

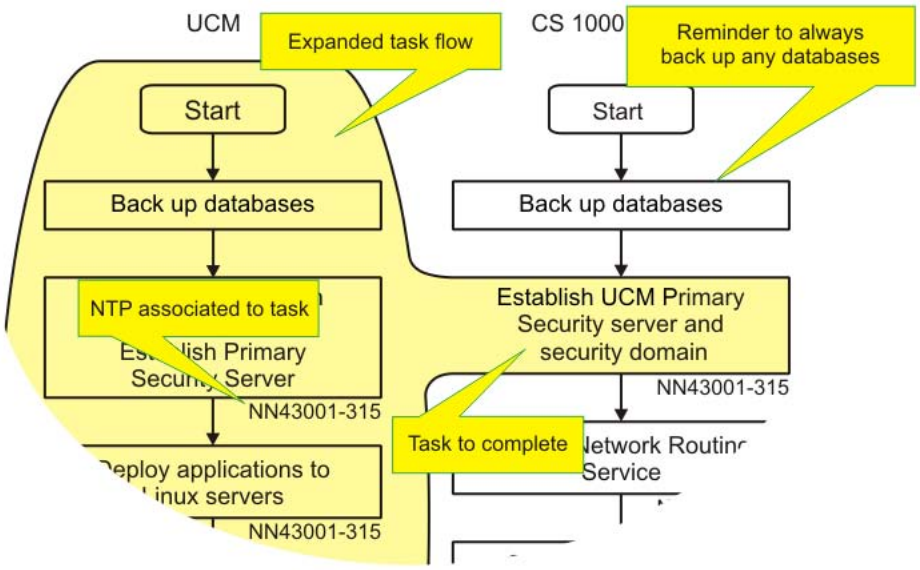

Figure 1: Example task flow

Referenced documents

The following documents are referenced in the task flow diagrams:

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

- *SIP Trunk Bridge Fundamentals , NN43001-143*
- *IP Peer Networking Installation and Commissioning , NN43001-313*
- *Communication Server 1000E High Scalability Installation and Commissioning, NN43041-312*

Network

Figure 2: Network task flow on page 20 appears in *Planning the Network-wide Upgrade, NN43001-406*.

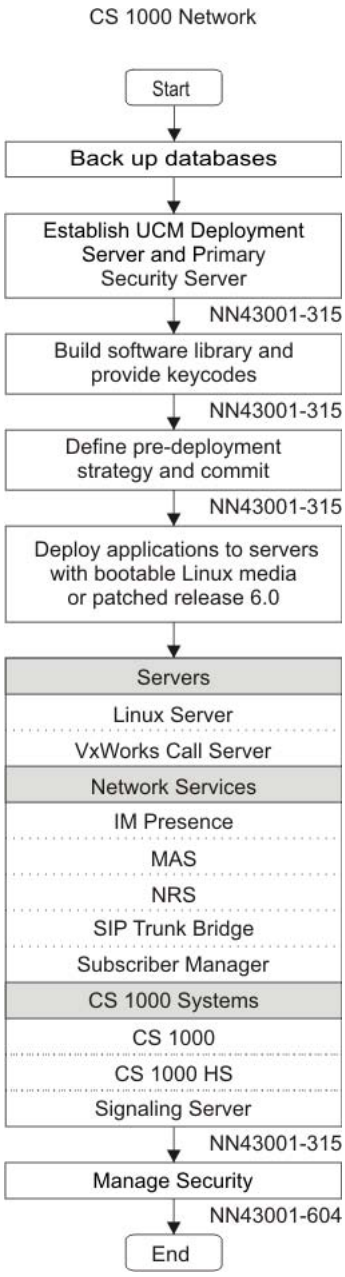

Figure 2: Network task flow

Linux base and UCM

Figure 3: Linux base and UCM task flow on page 21 appears in *Linux Platform Base and Applications Installation and Commissioning, NN43001-315* and *Unified Communications Management Fundamentals , NN3001-116*.

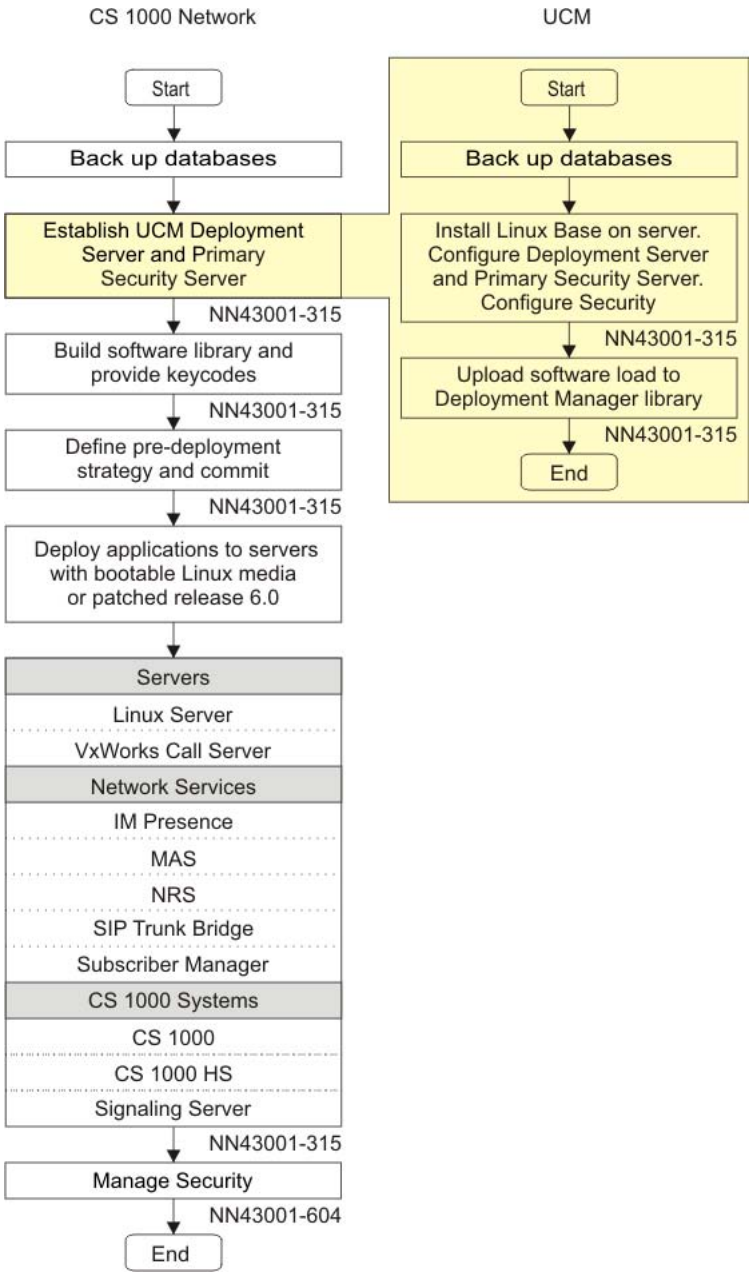

Figure 3: Linux base and UCM task flow

Network Routing Service

Figure 4: Network Routing Service task flow on page 22 appears in *Network Routing Service Fundamentals, NN43001-130*.

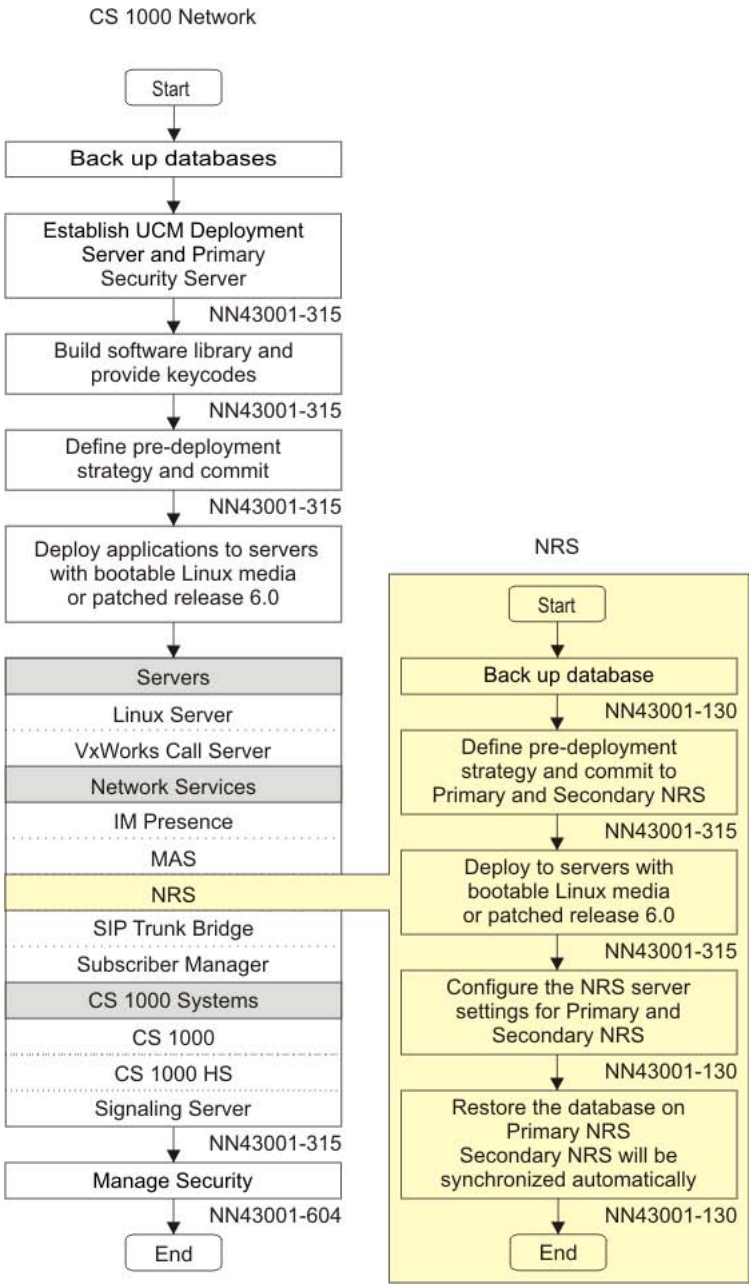

Figure 4: Network Routing Service task flow

CS 1000E High Availability

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

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

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

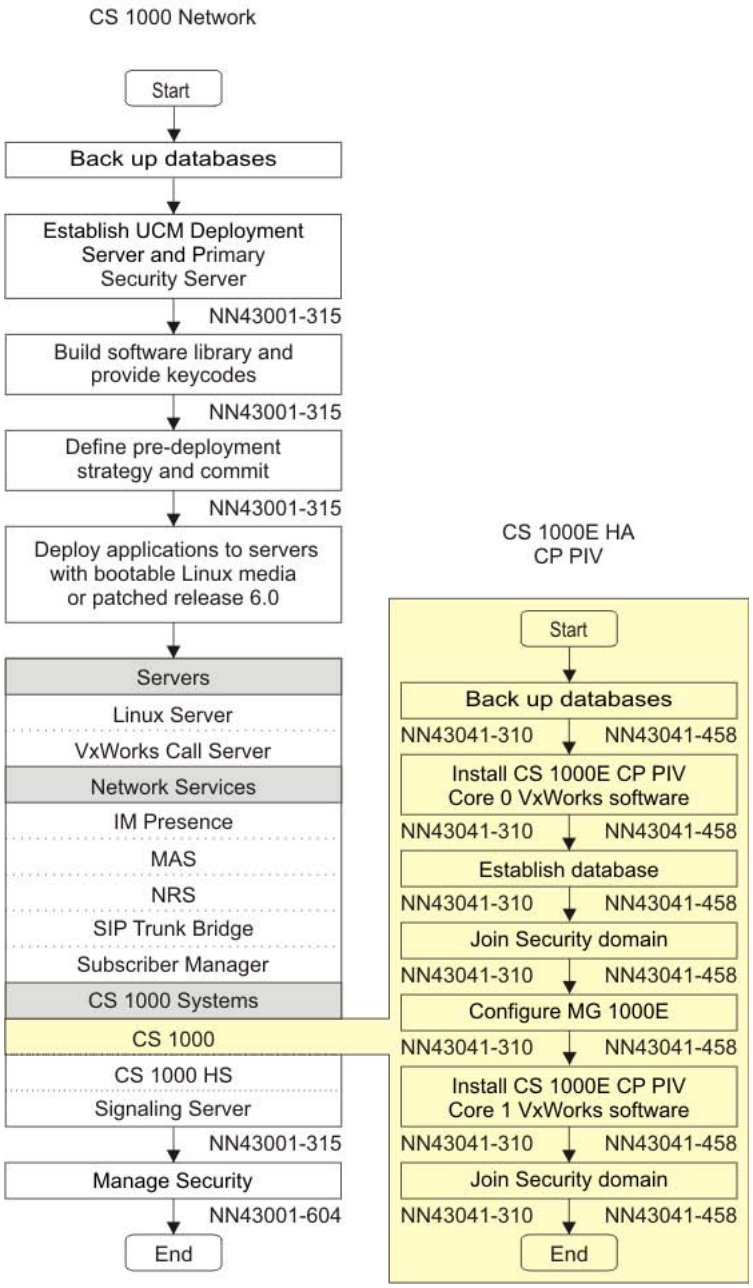

Figure 5: CS 1000E HA CP IV task flow

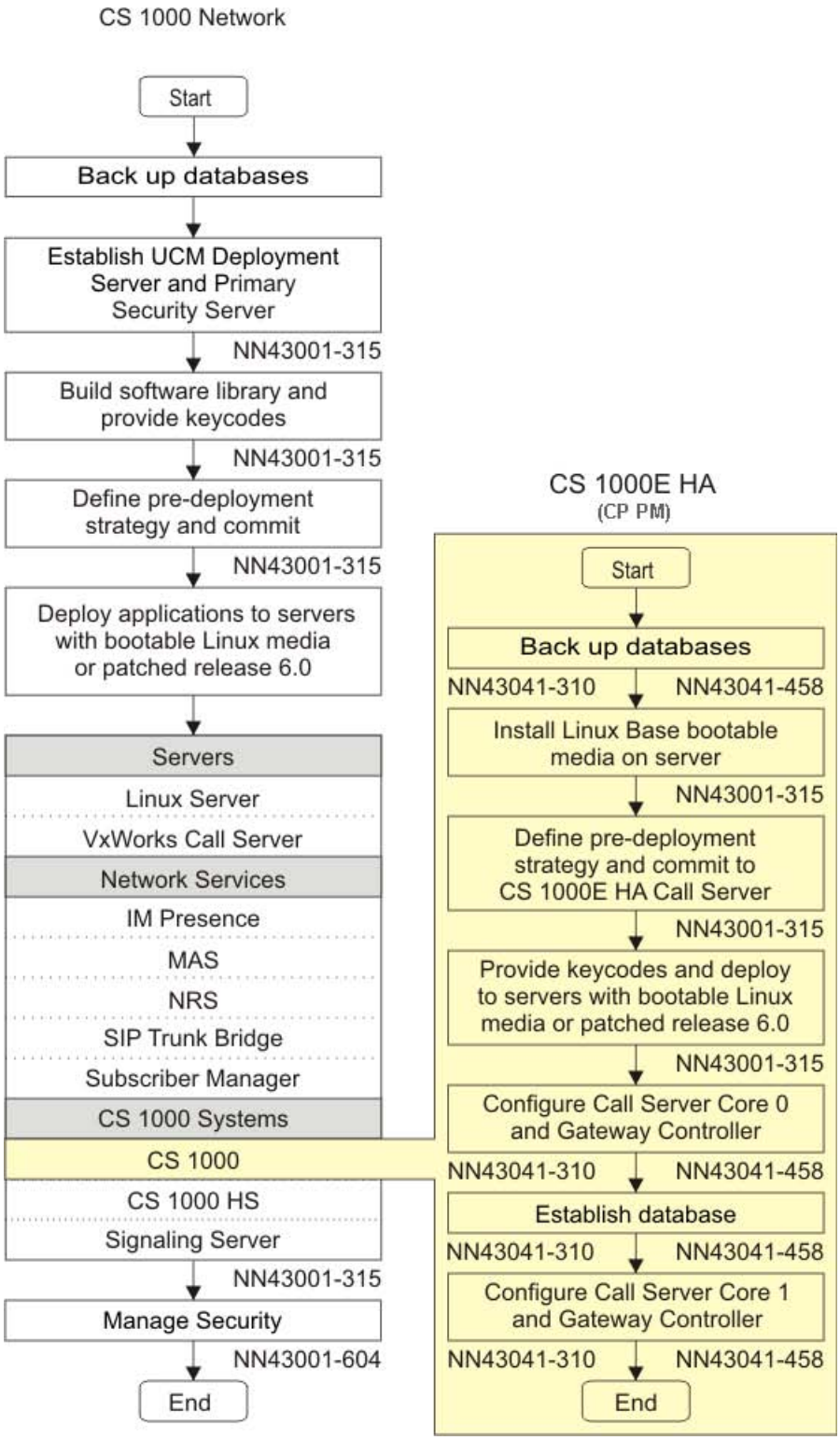

Figure 6: CS 1000E HA task flow

CS 1000E Co-res

Figure 7: Co-res task flow on page 26 appears in *Co-resident Call Server and Signaling Server , NN43001-509*.

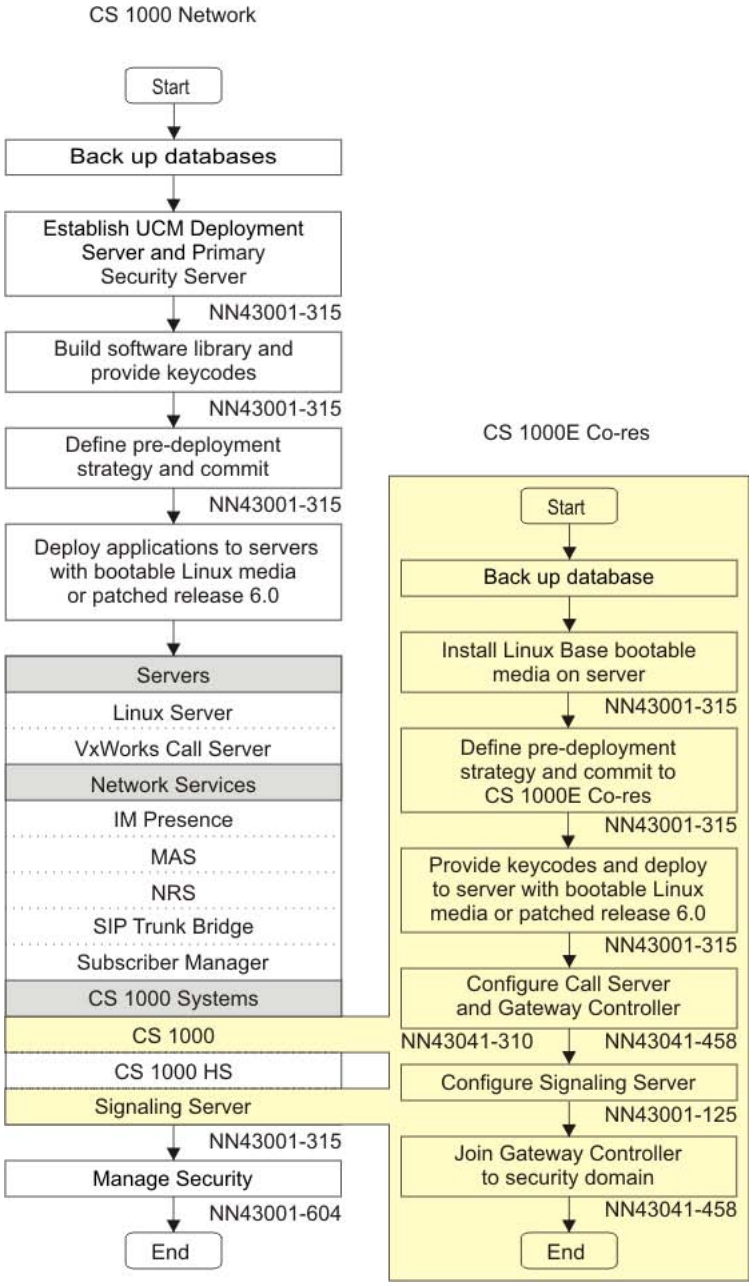

Figure 7: Co-res task flow

CS 1000M

Figure 8: CS 1000M task flow on page 27 appears in *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning , NN43021-310* and *CS 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*.

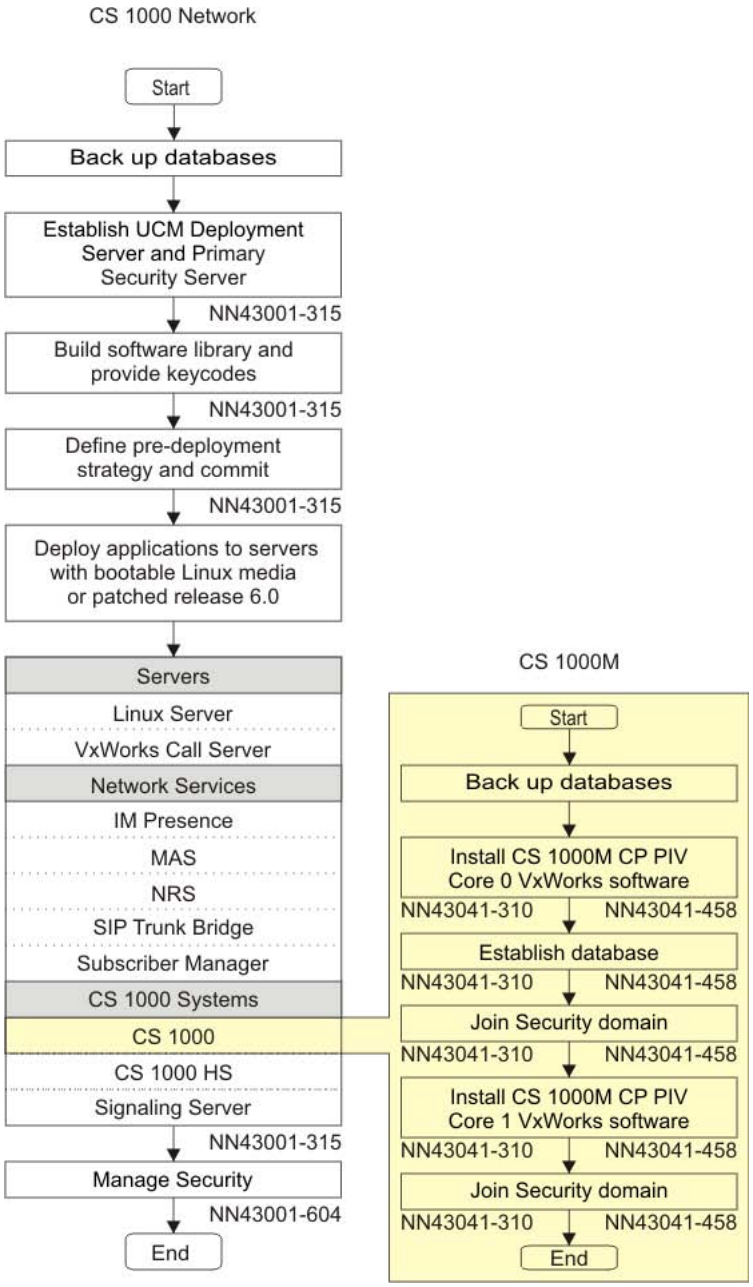

Figure 8: CS 1000M task flow

Signaling Server

Figure 9: Signaling Server task flow on page 28 appears in *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

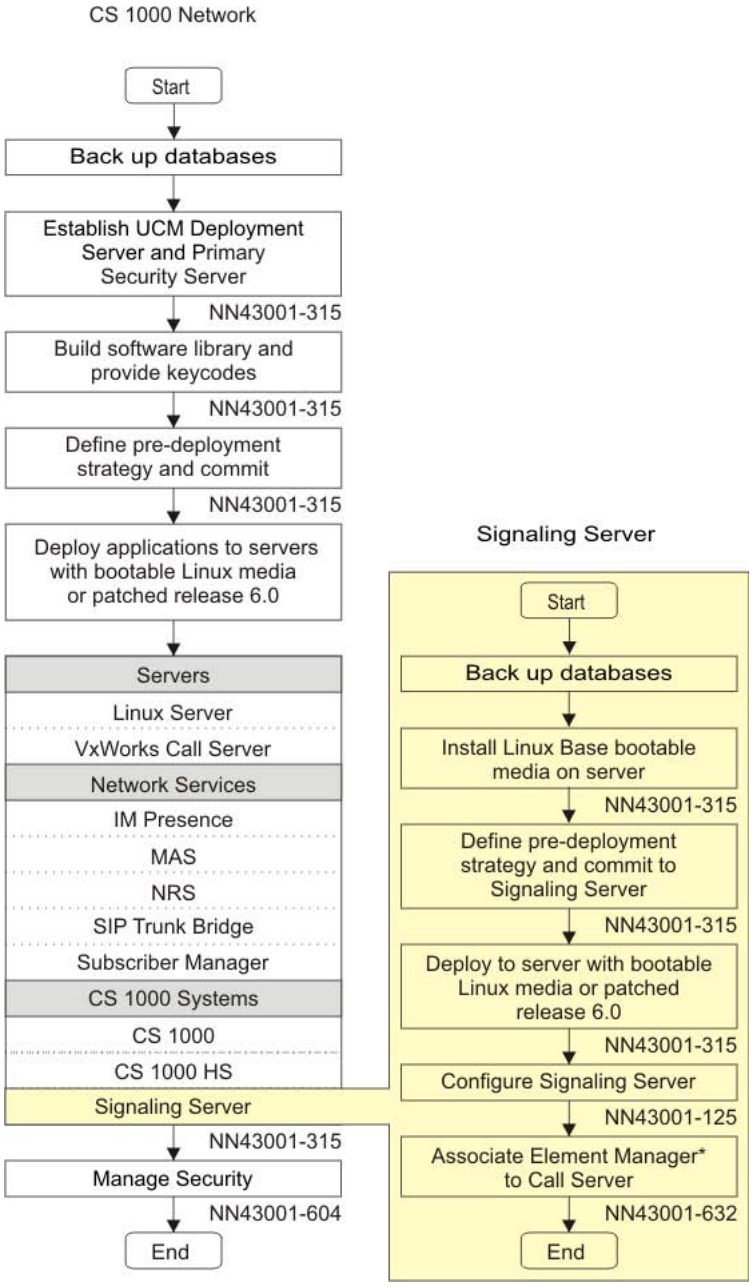

Figure 9: Signaling Server task flow

Branch Office

Figure 10: Branch Office task flow on page 29 appears in *Branch Office Installation and Commissioning , NN43001-314*.

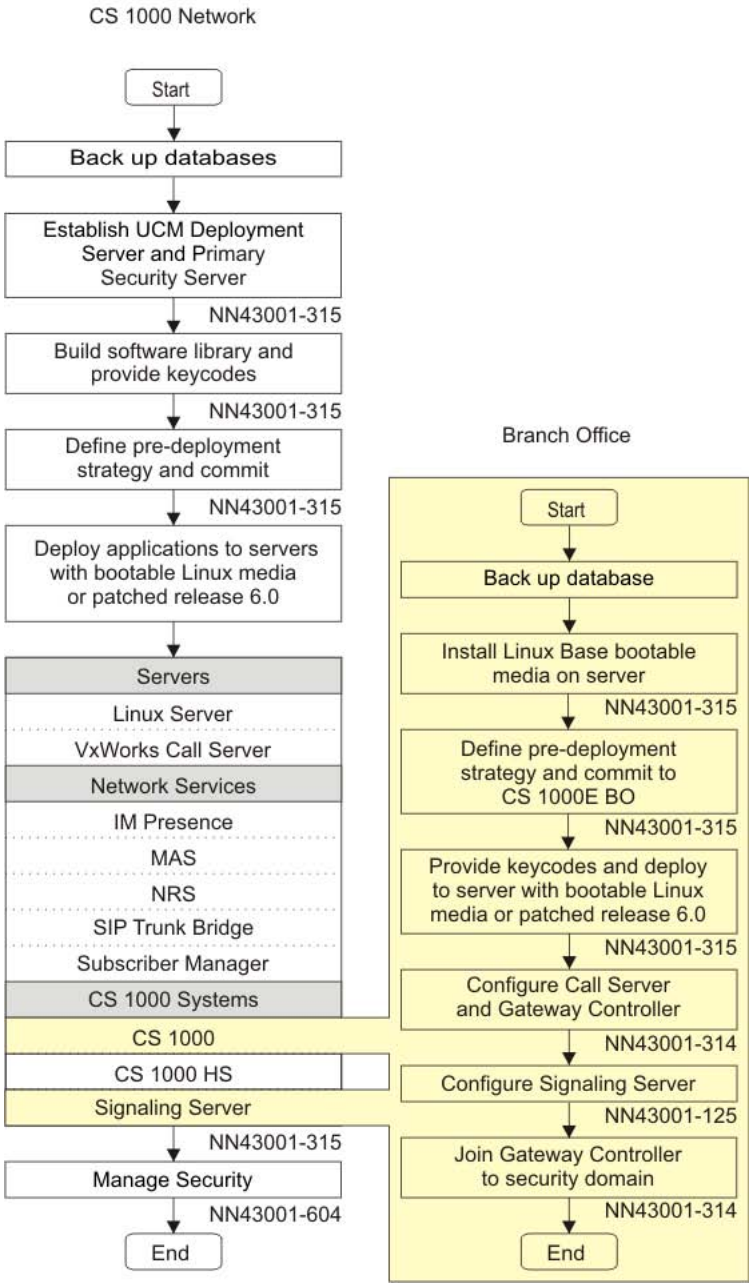

Figure 10: Branch Office task flow

SIP Line

Figure 11: SIP Line task flow on page 30 appears in *SIP Line Fundamentals, NN43001-508*.

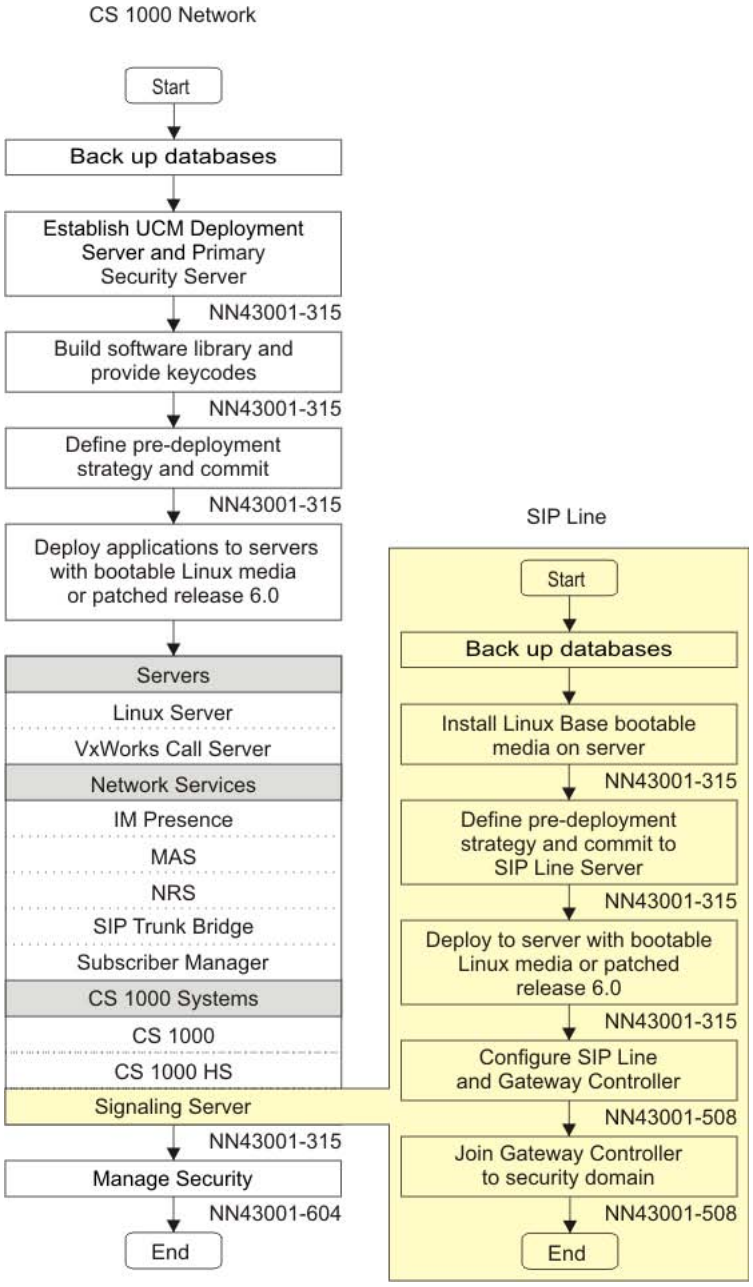

Figure 11: SIP Line task flow

SIP Trunk Bridge

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

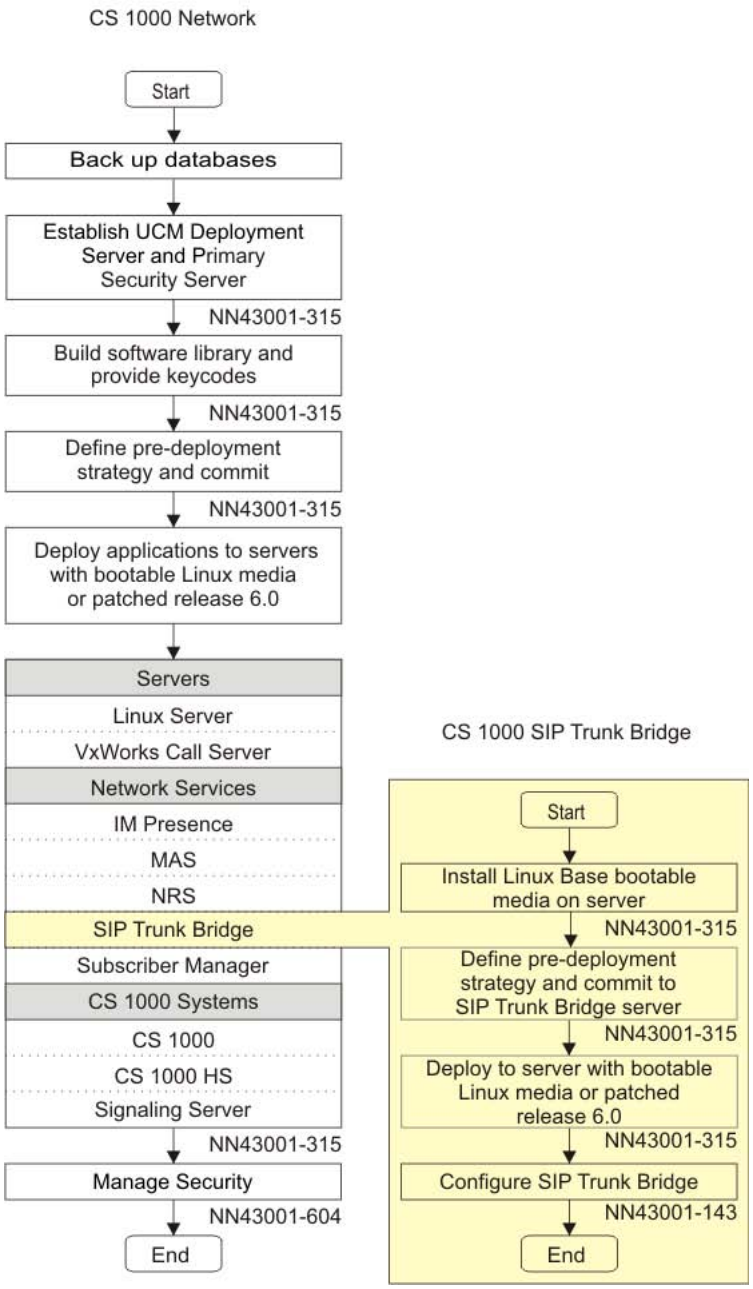

Figure 12: SIP Trunk task flow

High Scalability

Figure 13: High Scalability task flow on page 32 appears in *Communication Server 1000E Planning and Engineering – High Scalability Solutions (NN43041-221)*.

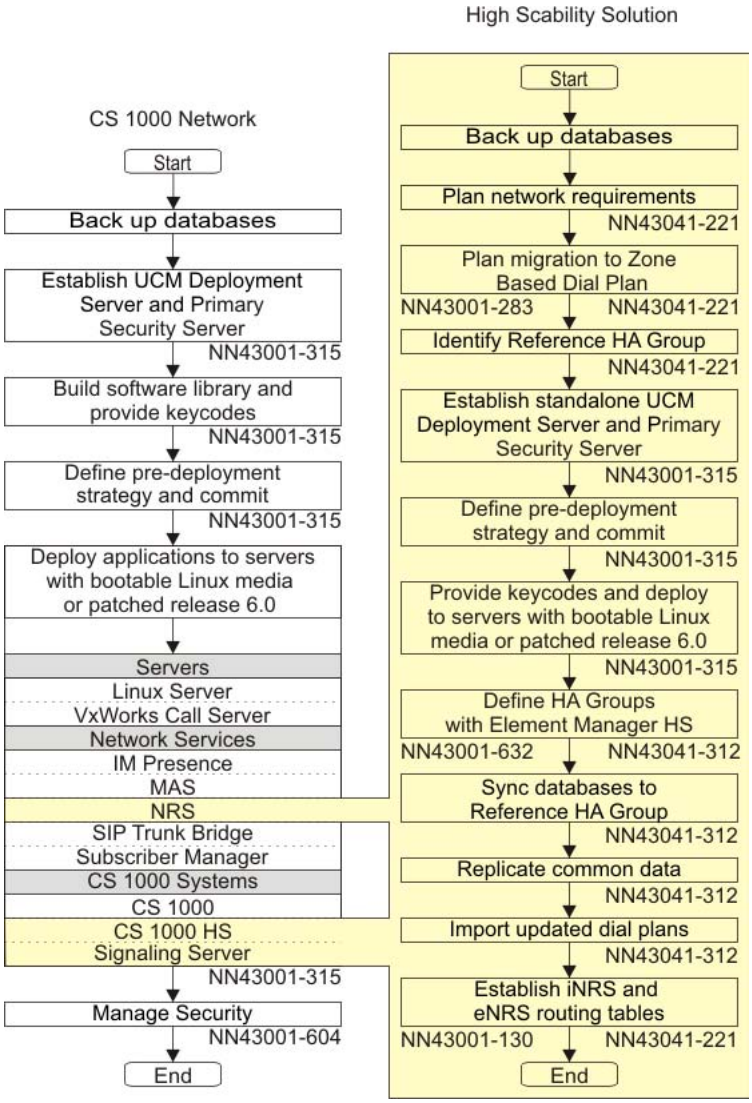

Figure 13: High Scalability task flow

Survivable SIP Media Gateway

Figure 14: Survivable SIP Media Gateway task flow on page 33 appears in *IP Peer Networking Installation and Commissioning , NN43001-313*.

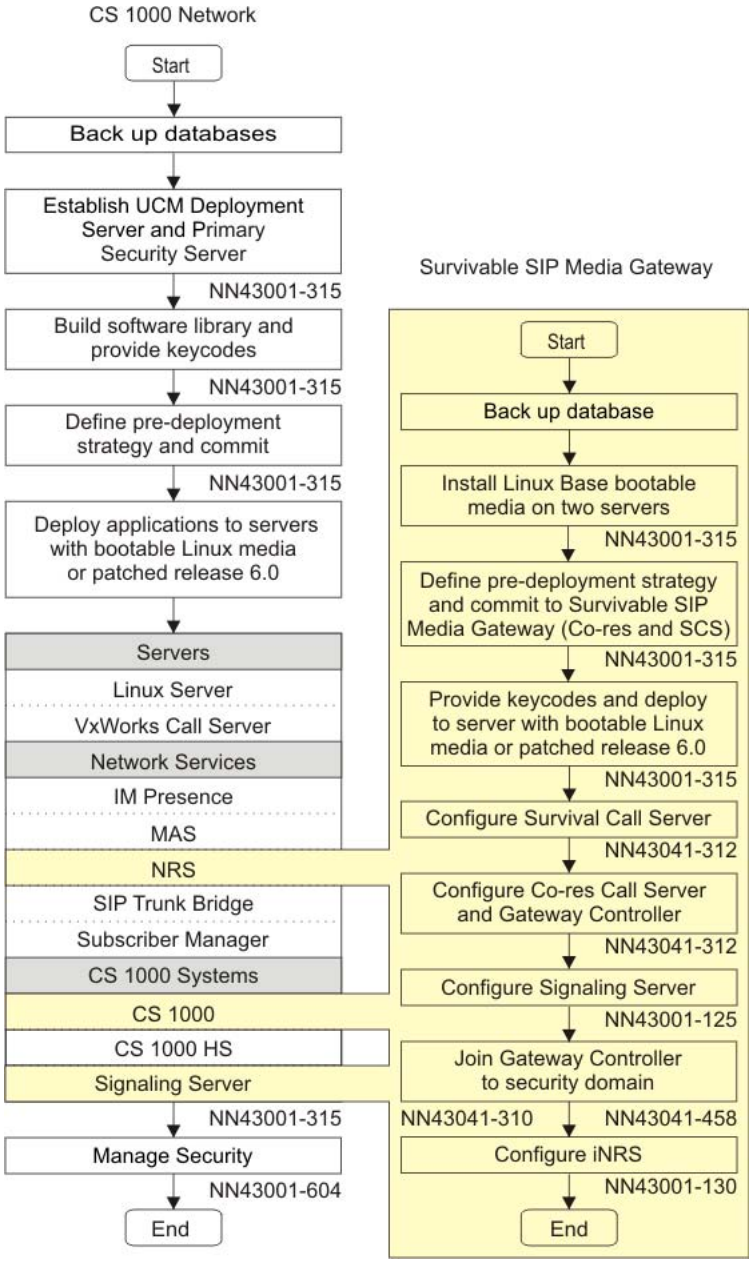

Figure 14: Survivable SIP Media Gateway task flow

Chapter 4: High Scalability system

Overview

The High Scalability (HS) system type provides you with a cost-effective solution that meets your increasing scalability needs. The Communication Server 1000E HS architecture leverages Communication Server 1000E High Availability (HS) systems and Network Routing Service (NRS) to achieve high scale and seamless intrasystem calling. By deploying HS, you can easily combine up to six Communication Server 1000E HA systems in a single, centrally-administered configuration. Use the Element Manager HS system management application as the single point administration tool to configure common data and unique user data for HS that is automatically propagated to each HA system in the solution. Using Element Manager HS saves time and effort, as you are no longer required to update individual HA systems. Some of the key benefits of Communication Server 1000E HS are:

- Leverages highly resilient and redundant Communication Server 1000E HA systems.
- Scales up to a combination of 150 000 IP endpoints and 36 000 TDM endpoints.
- Enables cost effective, simple, and centralized system management through the Element Manager HS.
- Element Manager HS automatically propagates common system data and unique user data to all HA systems in the HS solution.
- Seamless intrasystem calling through the NRS.

System deployment models

There are three types of deployment models:

- Campus Redundancy
- Geographic Redundancy
- Multiple HA groups dispersed geographically

Management Tools

The high-scalability solution offers enhanced management tools to provide central management capabilities for supporting multiple Communication Server 1000 groups. The

enhanced tools reduce the administrative effort of common data and ensure new information or updates occur only once and propagate to all HA groups. The following is a list of the High Scalability management capabilities:

- Deployment and installation of components including Call Server, Network Routing Servers (NRS)
- Unified Communications Management (UCM): Hierarchical tree grouping of elements under a Communication Server 1000 system
  - Manage Access control based on the hierarchical grouping of elements
  - Manage Deployment Manager, Patching Manager, and SNMP configuration using the hierarchical grouping of elements
- UCM: Group elements by geographic location
- Subscriber Manager/Phone configuration
- Numbering plan and dial plan management: automatic population of NRS and Call Server
- Element Manager: propagates common data to appear as a single entity from a management perspective
- Fault Management: features for managing faults, configuration, accounting, and performance measurement and security (FCAPS) are supported on individual servers

Unified Communications Management

The tree view shows a Communication Server 1000E HS system including all elements, and expands to show the related HA groups (including the associated Call Server, Signaling Servers, Media Gateway Controller (MGC), and Media Cards). In addition to showing the related HA groups, the tree view can be used to group systems by geographic location to identify the geographic redundancy and HA relationships in a related HA group.

Element Manager

You can navigate the hierarchy of components in Element Manager using a single sign-on. You can efficiently and consistently access and manage various elements within the network. Element Manager centralizes and simplifies configuration of individual HA groups that constitute a Communication Server 1000E HS system.

Element Manager for an HA group can:

- list individual HA groups that are part of the Communication Server 1000E HS system
- identify all the data that is considered common to the HS system and push the updates to the individual HA groups
- update data that is specific to an HA group by selecting the group from the list and performing the relevant operation

Deployment Manager

Use Deployment Manager to install all components (except VxWorks-based Call Servers) for an HS system. Deployment Manager is installed on the Primary Security Server. Deployment Manager provides a simple and unified solution that enables network installation of Linux Base and applications. Deployment Manager is used to create the group view for HS and deploy the components. For more information about Deployment Manager, see Linux Platform Base and Applications Installation and Commissioning (NN43001-315).

SNMP Profile Manager

The SNMP Profile Manager Profile Distribution page is enhanced for HS systems by displaying a list of system nodes in a tree view format. This allows you to select multiple nodes for profile distribution. Top-level nodes can be expanded to show the individual elements assigned to each node. Selecting a primary node causes the secondary nodes to be selected automatically. You can select up to a maximum of 500 elements for profile distribution.

For more information about SNMP Profile Manager, see *Fault Management—SNMP, NN43001-719*.

Subscriber Manager and phone provisioning

At the network security domain level, the Subscriber Manager application interacts with Element Manager (EM) for Communication Server 1000E HS systems and EM for individual Communication Server 1000 systems.

The phone provisioning component for a Communication Server 1000E HS Element Manager supports templates that you can use across multiple constituent HA groups. You do not have to explicitly export them from one group for importing to another.

Numbering Plans

A numbering group represents a common numbering plan. The numbering plan attributes (such as DN range, country code, area code, exchange code, private network identification, customer number, and Layer 0 (L0) domain name) are shared by a group of subscriber telephony accounts. You can define a numbering group to include numbering zones on the Call Server. The numbering groups also can automatically create and delete NRS entries that correspond to the number ranges that are entered.

System management reliability and redundancy

The model for system management reliability and redundancy for High Scalability provides a writable Primary security server and a read-only Backup security server. The Primary security server provides authentication/authorization, element registry lookup, user management, element registration, certificate management, IPsec management, SNMP configuration, centralized deployment, centralized patching, and subscriber manager functions for the Primary security server. The Backup security server performs element authentication and registration, if the Primary security server is unreachable.

In situations where both the Primary and Secondary servers are unreachable, Element Manager (EM), Deployment Manager and Patch Manager can be started and used on a local system. Command Line Interface (CLI) access is also available.

Unified Communication Manager navigation and access control

You can use Unified Communication Manager (UCM) to assign access control permissions to a single Communication Server 1000 system or to a High Scalability (HS) system as one entity to simplify administrative effort. You can manage common data for all systems that are part of the HS system so that new information or updates are done only once. You can also manage data that is specific to an individual HA group.

IPSec robustness and scalability

IPSec provides security at the ISSS level using either OPTI or FULL settings. High Scalability enhancements include:

- Support for IPSec Dead Peer Detection (DPD) for improving detection time of loss of IPSec connectivity between peers and resulting packet loss in certain scenarios.
- Changing from exclusive use of 3DES encryption to using AES128 with an secondary choice of 3DES. This change provides increased performance during encryption/ decryption of packets as well as higher security. 3DES continues to be available for compatibility with interfacing to other systems.
- Performance of the platforms in loading IPsec policies following system restarts and after changing the ISSS levels provides higher scalability.
- Some IPSec policies are improved to remove overhead and improve security in certain situations.

ISSS management scalability

The number of elements in the UCM security domain have increased beyond 1000 for a Communication Server 1000E HS system. The following enhancement applies to limiting the scope for ISSS management:

- Reduction to the maximum time for data distribution by changing the scope of management for ISSS. Changes propagate to the affected elements to limit the scope to High Scalability (HS), Geographic Redundancy (GR), or individual Communication Server 1000 system or gateway.
- Limit the scope of manual ISSS targets to a single system (HS, GR, or individual Communication Server 1000 system or gateway).
- Manage ISSS levels and pre-shared keys at a HS, GR, or individual CS 1000 system or gateway level, rather than the entire security domain.
- Restrict management of ISSS settings for a given system (HS, GR, or individual Communication Server 1000 system or gateway) to users with privileges to manage ISSS on that system.

Scalability

Overall scalability has increased with the Communication Server 1000E High Scalability solution. The following sections describe the changes.

SMG scalability

The High Scalability solution provides support for a maximum configuration of 50 Survivable Media Gateways (SMG) for every Communication Server 1000 system. Changes include a reduced load on the Call Server when transferring database files from the Call Server. These changes reduce impacts on other Call Server applications during database transfers and increase the robustness of these transfers when you deploy a larger number of SMGs.

Survivable SIP Media Gateway—Geographic Redundancy

In CS 1000 Release 7.0, a Geographic Redundancy model introduces the concept of the Survival SIP Media Gateway (SSMG) . The Survivable SIP Media Gateway architecture removes the restriction of the 80 millisecond Round Trip Delay (RTD) in the Geographic Redundant network and allows the Primary Call Server to support up to 511 Secondary servers in a GR N-way model.

The Survivable SIP Media Gateway is a new deployment option which separates the Survivable Server from the Media Gateway component. The Survivable SIP Media Gateway architecture consists of a Communication Server 1000E system configured as a Survivable Server (GeoSecondary package is enabled) and a Communication Server 1000E TDM system configured as the SIP Media Gateway. These two systems are usually co-located in the same chassis. The choice of hardware is dictated by the number of users at the location which the Survivable SIP Media Gateway serves. The CP DC card is recommended as the Survivable Server platform and the CP MG card is recommended for the SIP Media Gateway. The CP DC and the CP MG typically run the co-resident CS+SS applications.

The Secondary Call Server component of the Survivable SIP Media Gateway provides Primary Call Server redundancy. In normal operation, all IP Phones at all locations register to the Primary call server. In the event of a WAN outage, the IP Phones register to the local Survivable SIP Media Gateway, specifically to the Secondary Call Server component of the Survivable SIP Media Gateway.

In the Survivable SIP Media Gateway model, the TDM resources on the CP MG card, the MGC and/or the Media Cards register to the SIP Media Gateway component. There is no redundancy available for TDM resources in this model. The local registration of TDM resources removes the 80 millisecond RTD restriction previously imposed for GR networks. This model also frees up TN space on the Primary Call Server because the TDM resources are no longer configured on the primary and there is no need to dedicate an entire superloop to the MGC card. Therefore, the Primary Call Servers can support up to 511 systems in survival mode.

The Geographic Redundancy data replication model remains unchanged from Release 6.0. The database configured on the Primary Call Server gets replicated to the Secondary Call

Server components of the Survivable SIP Media Gateways in the network. The database on the SIP Media Gateway is configured independently.

UCM registration robustness and simplification

The following enhancements improve the robustness and operation of UCM registration:

- Automatic updates for distributing ISSS data for Communication Server 1000 elements when registering or unregistering from the UCM security domain. Other benefits include a reduction in the manual steps and involvement of multiple roles.
- Automatic provisioning of Media Gateway Controller and Media Cards to initialize with the Call Server prior to registration with UCM when ISSS is at OPTI or FULL levels. Manual steps during installation and replacement of Media Gateway Controllers and Media Cards are eliminated.
- Provides an automatic mode of registration to the UCM security domain for Media Gateway Controllers and Media Cards for systems not requiring the highest levels of security. Provisioned Media Gateway Controllers and Media Cards are automatically trusted and registered with the security domain when they contact the Call Server.
- Improvements to the internal operation of the UCM registration process for High Availability (HA) Call Servers, Media Cards and Media Gateway Controllers ensure a more robust operation.

Element Manager

Element Manager has been enhanced to improve the overall performance and scalability. Response time and throughput of the interface have increased.

Personal Directory scalability

The existing Personal Directory application has been enhanced to provide the scalability and robustness required for HS systems.

Network Routing Service

A tertiary Network Routing Service (NRS) server is introduced and provides a third level of redundancy for the SIP Gateway (SIPGW) and compliments the existing Failsafe operations. This third level provides improved flexibility and ease of deployment for an HS solution. The tertiary NRS can run on any device on the network and operates in a point-to-point mode. The

tertiary NRS provides more flexibility because it has an independent NRS database that is tailored to route SIP calls during a WAN outage scenario. For more information about the Tertiary NRS server, see *Network Routing Service Fundamentals (NN43001-130)*.

SIP Trunk and SIP Line

Enhancements to increase the SIP Trunk and SIP Line application for the number of supported ports from 1800 to 4000 for each Signaling Server and support for 8000 telephones on a single server (with some blocking).

IP Line

Enhancements to improve the registration time of IP Phones has been made.

Call Server scalability

Enhancements to increase the capacity of a single call server to 40 000 telephones. With this increase, almost all customer sites are supported on a single Call Server, thus avoiding potential issues with feature transparency when users are on different Call Servers. Modifications to the Incremental Software Management (ISM) tools provide licensing for increased capacities. You can move user licenses between Call Servers of a HS system without the inconvenience and risk of major disruption caused by reloading the system.

More information

For more information about planning and engineering a high scalability solution, see *Communication Server 1000E Planning and Engineering – High Scalability Solutions (NN43041-221)*.

For more information on deploying a high scalability solution, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

For more information about migrating to a high scalability solution, see *Communication Server 1000E High Scalability Installation and Commissioning, NN43041-312*.

Chapter 5: IP Media Services

Overview

IP Media Services provides Communication Server 1000 systems with IP versions of traditional TDM-based media services, such as Conference, Music, RAN, Tone, and Attendant Console, by using the Nortel Media Application Server (MAS) as the IP media service delivery platform.

The MAS supplies media services by using both secure and non-secure Real-time Transport Protocol (sRTP and RTP) channels controlled by the Call Server and Signalling Server, which map the MAS resources to existing virtual TNs. The MAS is an IP-based media server and does not require DSPs for delivering IP media services to IP endpoints.

Note:
IP Media Services is only supported for CS 1000E systems.

The IP Media Services applications are included with the Signaling Server software and deployed as part of Signaling Server installation. IP Media Services includes the following features and applications:

- IP Ad Hoc Conference
- IP Music Broadcast
- IP Recorded Announcements
- IP Tone Generation
- IP Attendant Console (3260)

For more information about the IP Media Services applications, see *Features and Services, NN43001-106*.

On the Call Server, the existing media service delivery standards are maintained. However, new IP-based media resource types emulate traditional TDM media resources and operate as virtual TNs, using software to replace former hardware functionality. The virtual TN-based resources are IP Ad Hoc Conference and IP Tone loops, as well as IP Music and IP RAN routes and trunks.

In systems where both TDM and IP-based resources are active, the Call Server selects the appropriate resource based on the service target. Music and RAN services are selected based on the route type defined in the Customer and Route Data Blocks and Conference service is determined by the caller who presses the conference key. Whenever possible, the Call Server selects the same media resource type as the service target.

As with other virtual TN services, application software on the Signaling Server replaces the functionality formerly provided by TDM hardware. IP Media Services introduces new

applications to the Signaling Server that act as the signaling bridge between the Call Server and the MAS servers. These applications receive the traditional TDM-based signaling from the Call Server using the existing Signaling Server PBX Link and direct the MAS signaling using SIP.

Each IP Media Services application acts as a collection of SIP clients. When the Call Server requests a media resource, the corresponding IP Media Services application creates a new SIP client, which then makes a SIP request to the MAS. Once the SIP session is established, the MAS negotiates a media path with the target endpoint in response to speech path control messages received from the Call Server.

MAS servers deliver RTP based media services to the IP endpoints based on instructions received from the Call Server and Signaling Server. The MAS servers are directed by SIP signaling from the IP Media Services controllers to deliver RTP service streams to IP endpoints and to subsequently tear down the streams upon completion of service delivery. IP Media Services supports both secure and non-secure RTP and TLS signaling for the media path.

The relationship of MAS servers to CS 1000E resources is flexible; one MAS can provide services to many Call Servers or several MAS servers can provide service to one Call Server, depending on the number of subscribers supported by the Call Servers.

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

Chapter 6: SIP Trunk Bridge

Communication Server 1000 SIP Trunk Bridge is a new application in the Communication Server (CS) 1000 network that provides SIP signaling mediation and media anchoring for SIP interoperability with SIP Trunk providers using Network Address Translation (NAT) traversal. You can deploy this application on three servers. Each SIP Trunk Service Provider connected from CS 1000 needs a dedicated SIP Trunk bridge (co-residency is not supported in this release) to inter-operate with the provider. SIP Trunk Bridge is available in either a stand-alone or redundant mode. Additional features such as support for mid-call feature capabilities which enhance Mobile X functions during connections to the Mobile Carrier through SIP trunk are also supported in this release.

For more information about SIP Trunk Bridge, see SIP Trunk Bridge Fundamentals (NN43001-143).

Chapter 7: New hardware

This chapter describes new hardware introduced in Communication Server 1000 Release 7.0.

Common Processor Media Gateway (CP MG) card

The Common Processor Media Gateway (CP MG) card is a new hardware platform for use in a Communication Server 1000E system. The CP MG card functions as a Server, a Gateway Controller, and provides Digital Signal Processor (DSP) resources.

Overview

The hardware for the CP MG card consists of integrating a Common Processor, a Gateway Controller, and non-removable DSP resources into a single card for use in a Communication Server 1000E system.

The CP MG card is available in two versions:

- NTDW56BAE6 - CP MG card with 32 DSP ports (CP MG 32)
- NTDW59BAE6 - CP MG card with 128 DSP ports (CP MG 128)

The CP MG card provides improvements in port density and cost reductions by functioning as a Call Server or Application Server and a Gateway Controller with DSP resources while only occupying slot 0 in a Media Gateway. The CP MG card supports all CS 1000 IPE cards, and supports the full suite of CS 1000 telephones.

The CP MG 32 is an ideal hardware platform for small Branch Offices with less than 100 users. The CP MG 128 is an ideal hardware platform for Branch Office and Co-resident Call Server and Signaling Server configurations with less than 800 users.

The Common Processor component of the CP MG card provides the Server functions. The Gateway Controller component of the CP MG card is based on the same architecture as the MGC card and uses the common MGC loadware. The Gateway Controller component of the CP MG card registers to the Server with an IPMG type of MGS.

The CP MG card requires the Linux base Operating System, and supports the Co-resident Call Server and Signaling Server, CS 1000E TDM, or stand-alone Signaling Server configurations. The CP MG card does not support the standard or high availability Call Server configuration.

CP MG specifications

The CP MG card includes the following main components:

- Intel EP80579 integrated processor, 1200 Mhz (Common Processor)
- 2 GB DDR2 RAM (expandable to 4 GB)
- 160 GB SATA hard drive (Server file system)
- Mindspeed Chagall-2 processor M82515 (Gateway Controller)
- Compact Flash card (ATA) (Gateway Controller file system)
- Mindspeed Picasso M82710 (32 port) or Matisse M82910 (128 port) DSP resources
- Embedded Ethernet switch (links the Server to the Gateway Controller)

The CP MG card faceplate provides a USB 2.0 port, two Server serial ports, two Ethernet ports, status LEDs, a four character display, and reset buttons. The CP MG card backplane provides two Ethernet ports, and three serial ports.

For more information about the CP MG card hardware components, see *Communication Server 1000E Circuit Card Reference, NN43001-311*.

Common Processor Dual Core (CP DC) card

The Common Processor Media Gateway (CP MG) card is a new hardware platform for use in a Communication Server 1000 system. The CP DC card functions as a Server in a CS 1000 system, and is designed to replace the existing Common Processor Pentium Mobile (CP PM) card.

Overview

The CP DC card contains a dual core AMD processor and upgraded components which can provide improvements in processing power and speed over existing Server cards. The CP DC card provides performance improvements in MIPS, maximum memory capacity, and network transfer rate, and occupies one IPE slot in a Media Gateway cabinet or chassis.

The CP DC card is available in two versions:

- NTDW53AAE6 - single slot CP DC card
- NTDW54AAE6 - double slot CP DC card

The NTDW53 CP DC card is designed for the CS 1000E Media Gateway. The NTDW54 CP DC card is designed for the CS 1000M IPE Universal Equipment Module (UEM).

The CP DC card is required for some new CS 1000 Release 7.0 applications, such as Media Application Server (MAS) and SIP Trunk Bridge. The CP DC card supports a Co-resident Call Server and Signaling Server configuration with less than 800 users.

The CP DC card requires the Linux base Operating System, and supports the Co-resident Call Server and Signaling Server, or stand-alone Signaling Server configurations. The CP DC card does not support the standard or high availability Call Server configuration.

CP DC specifications

The CP DC card includes the following main components:

- AMD Athlon 64 X2 1.8 Ghz dual core processor
- 2 GB DDR2 RAM (expandable to 4 GB)
- 160 GB SATA hard drive (Server file system)
- Three faceplate USB 2.0 ports (for installations, upgrades, patches, and USB keyboard and mouse support)
- One faceplate VGA port (monitor support)
- Two faceplate Gigabit Ethernet ports
- Faceplate status LED and card reset buttons

For more information about the CP MG card hardware components, see *Communication Server 1000E Circuit Card Reference, NN43001-311*.

128 port DSP daughterboard (DB-128)

The 128 port DSP daughterboard (DB-128) is a new Media Gateway Controller (MGC) card daughterboard. The MGC card supports the DB-32, DB-96 and DB-128 daughterboards. The MGC card can now support a maximum of 256 DSP ports.

Overview

The NTDW78AAE6 128 port DSP daughterboard provides an MGC card with 128 DSP ports while occupying only one of the two MGC card expansion site. New MGC cards ship populated

with one DB-128. Previous to DB-128, an MGC card with 128 DSP ports required the expansion sites to be populated with a DB-32 and a DB-96.

The DB-128 is supported in both expansion sites on the MGC card. The DB-128 in expansion site 1 uses card slots 11, 12, 13, 14. The DB-128 in expansion site 2 uses card slots 0, 9, 10, 15.

DB-128 card slots are not dedicated. For example, you can configure card 9 and 10 for other card types when card 0 is configured as DB-128. Similarly, you can configure card 14 or card 15 for DTR/XTD when card 11,12, and 13 is configured as DB-128

The CS 1000E Peripheral Rate Interface (PRI) Media Gateway (PRI Gateway) can support a MGC card populated with two DB-128 for a maximum of 256 DSP ports. The Extended Media Gateway PRI (MGP) package 418 is required to support MGC cards populated with greater than 192 DSP ports.

For more information about the DSP daughterboard components, see *Communication Server 1000E Circuit Card Reference, NN43001-311*.

Chapter 8: Deployment Manager enhancements

Deployment Manager on the Primary security server has been enhanced for CS 1000 Release 7.0 to provide for an end-to-end installation and configuration of Linux Base and applications. Deployment Manager provides a simplified and unified solution that enables network installation of Linux Base on target servers. The Primary security server is the Deployment Server.

Install the Linux Base on the Primary security server (Deployment Server) using a local Linux Base installation media. Upgrade Linux Base on the Member and Backup servers over the network using Network File System (NFS).

After installation and configuration is complete:

- Linux base is installed
- Base applications are installed during the first restart of the computer
- UCM is deployed and security configuration is complete
- The application combination is determined and deployed
- Applications are active

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

Chapter 9: Element Manager enhancements

Communication Server (CS) 1000 Release 7.0 brings significant key performance improvements to the Element Manager. New capabilities added include the configuration through Element Manager of many lists such as speed call, system speed call, group hunt and group call; and displays historic and current traffic data. CS 1000 Release 7.0 also supports increased coverage of Communication Server 1000 core features that includes new Media Services, SIP Trunk Bridge and High Scalability.

Lists

The CS 1000 Release 7.0 list feature enables the customer to create, view, edit, and delete lists in Element Manager. Customers can add and modify lists through a comma-separated value (CSV) file or a web detailed interface, and also import new lists into the system in the CSV format.

For more information about Lists, see *Element Manager System Reference - Administration, NN43001-632*.

Traffic

The CS 1000 Release 7.0 traffic feature enables the customer to collect traffic data on the system, enable or disable a specific traffic report, and view the historic and current traffic records. The reports are collected every 30 minutes and are stored locally. The customer can view the historic and current records by clicking on the corresponding report type.

For more information about Traffic, see *Element Manager System Reference - Administration, NN43001-632*.

Electronic Switched Network data and Maintenance commands

In this release, Electronic Switched Network (ESN) data and Maintenance commands can both be managed through Element Manager.

For more information, see *Element Manager System Reference - Administration, NN43001-632*.

Chapter 10: Subscriber Manager enhancements

Overview

Communication Server (CS) 1000 Release 7.0 includes many new and enhanced features for Subscriber Manager. For more information about Subscriber Manager, see *Subscriber Manager Fundamentals (NN43001-120)*.

Account delete when account does not exist in the element

Previous releases of Subscriber Manager required the user to run the Account Synchronization feature to remove accounts that no longer exist in the element. Account deletion in Subscriber Manager is enhanced so that these accounts can be easily deleted from the Subscriber Details web page. In previous releases, if a user attempted to delete an account that no longer existed in the element, they received an error message indicating that an internal error was encountered in the element, and so the account could not be deleted.

Accounts hidden based on access rights

Accounts that a user does not have access to are not displayed in the Subscriber Details Web page. A user does not have access to an account if the account is on an element that is not mapped to a security role the user is assigned.

Account migration

When synchronizing accounts for CallPilot elements, if the first and last name of the account match an existing subscriber, that account is automatically added to that subscriber. Note that the first and last name must match exactly, including case.

Automatic refresh on the Flow Through Provisioning status page

The following fields on the Flow Through Provisioning Web page are refreshed every three seconds:

- Processing status
- Processed from directory
- Processed subscriber change notification
- Last run completed
- Next run in

It is no longer necessary to manually refresh the web page.

Automatic mapping of location and template based on FTPROV configuration

Flow Through Provisioning provides configuration options for the user to map location and template to any of the subscriber properties. From the perspective of Flow Through Provisioning, the subscriber properties are used only if the provisioning request has not specified a location and/or template.

Automatic mapping of location and template also occurs when the user adds accounts through the Subscriber Manager user interface.

CallPilot Element Type

A CallPilot Messaging element type is available to be added from the Unified Communications Management (UCM) Common Services elements table. For more information, refer to Unified Communications Management Common Services Fundamentals (NN43001-116).

Because CallPilot is not integrated into the UCM Common Services security framework, in some cases additional sign on will be required.

Invalid accounts

An invalid account is defined as an account that does not have a valid Element in the Elements table in UCM Common Services. Invalid accounts are automatically removed from Subscriber Manager as they are discovered. Invalid accounts are not displayed in the Subscriber Manager user interface

LDAP synchronization status message enhancements

The synchronization status message is enhanced to indicate that the synchronization job name that has finished and the total number of entries that were available to be synchronized.

Messaging account assign or reassign

When a Messaging Account is assigned or reassigned to a subscriber, only the first name, last name and subscriber ID are updated in CallPilot. The mailbox number, extension DN and callback DN fields are not changed.

Messaging account synchronization

When a Messaging Account is synchronized using the Subscriber Manager Account Synchronization feature, the template information for that account is lost since CallPilot Manager does not store this information. As a result, the Template cell in the Accounts table is empty after the synchronization. If any of the mailbox properties are changed in CallPilot directly, performing an account synchronization operation only updates the service information for the account.

CallPilot does not support automatic synchronization to Subscriber Manager, unless the user launched CallPilot Manager through the Subscriber Manager Subscriber details Web page.

Numbering group feature removed from Subscriber Manager

In this release, the numbering group feature is removed from Subscriber Manager. For more information on the numbering group feature see *Signaling Server IP Line Applications Fundamentals (NN43001-125)*.

Scheduler

Use the Scheduler branch of the Subscriber Manager navigator to manage scheduled jobs.

Schedule the date and time for adding an account

In CS 1000 Release 7.0, the user has the option to schedule the date and time for adding a subscriber account .

Search by Unique User ID

There are three features in Subscriber Manager to quickly and easily search for subscribers within your network: (1) basic search, (2) advanced search, and (3) unique ID search. Basic and advanced search are preexisting features. The unique ID search is new in this release.

Subscriber Manager license

Subscriber Manager is no longer a separately licensed product.

Troubleshooting

See the Troubleshooting chapter in *Subscriber Manager Fundamentals (NN43001-120)* for information on adding a CallPilot SSL certificate on the UCM Common Services server.

Chapter 11: IP Line enhancements

Overview

Communication Server (CS) 1000 Release 7.0 introduces many new and enhanced features for IP Line. For more information about IP Line enhancements, see *Features and Services Fundamentals, NN43001-106*.

Disable Mute function on IP Phones

This feature allows administrators to disable the mute function of the IP Phone. If the mute function is disabled, then pressing the mute key places the active call on hold, rather than creating a one-way speech path. To take the call off hold, the user presses the mute key again or can press the DN key.

For more information, see “IP Phone Disable Mute function” in *Features and Services Fundamentals, NN43001-106*.

Last number redial soft key on IP Phone 1210

CS 1000 Release 7.0 introduces Last Number Redial (LNR) functionality for the IP Phone 1210 through a LNR soft key. This key is displayed when the IP Phone 1210 goes off hook. This soft key for IP Phone 1210 is allowed (denied) depending on the CLS LNA (LND) in LD 11 for the IP Phone 1210.

For more information, see “IP Phone 1210 Last Number Redial soft key” in *Features and Services Fundamentals, NN43001-106*.

Password protection for language and feature key label changes on IP Phone Services menu

This feature password-protects access to language and feature key labels changes in the Services menu of the IP Phones. If Controlled Class of Service (CCOS) is enabled and a Station Control Password (SCPW) is defined, the IP Phone requires the SCPW to access the Language menu and the Change Feature Key Label menu.

For more information, see “IP Phone Password Protection for Language and Feature Key Labels” in *Features and Services Fundamentals, NN43001-106*.

Callers List and Redial List display number instead of displaying unknown

Caller names and DN, and redial names and DN, are stored in the Callers List/Redial List after receiving or making a call. If a name is undefined, only the DN is displayed in the lists

Log incoming calls when IP Phone is busy

The IP Phones that support Callers List can configure the Callers List to log all incoming calls including calls while the IP Phone is busy. This feature is enabled through the Telephone Options menu.

Audio Message Waiting Indication (MWI) on IP Phones

The IP Phone Audio Message Waiting Indication feature supports audio-based Message Waiting Indication (MWI) for IP Phones. Audio-based MWI is configured for IP Phones with Message Waiting Tone Allowed (MWTA) in Element Manager.

For more information, see “IP Phone Audio Message Waiting Indication” in *Features and Services Fundamentals, NN43001-106*.

Virtual Office login and logout soft key display

This feature displays a soft key on the IP Phone to provide easy access to Virtual Office login/logout functionality. When the IP Phone is idle, a ‘Virtual’ soft key is displayed if the VOLA class of service is enabled.

When the IP Phone is registered to the home TN as a regular phone, the user can press the ‘Virtual’ soft key to log in to Virtual Office. If that IP Phone is logged in, using Virtual Office, to another IP Phone, and the ‘Virtual’ soft key is pressed, that IP Phone automatically registers to the home TN.

Virtual Office-only IP Phones

This feature allows an administrator to configure Virtual Office-only IP phones. These IP Phones are in a Virtual Office logout state by default; they do not have an assigned DN and they do not consume a TN license. These IP Phones can be used for only for Virtual Office login.

For more information, see “Virtual Office-only IP Phones” in *Features and Services Fundamentals, NN43001-106*.

Virtual Office logout during midnight routines

This feature allows automatic logout during the midnight routines of inactive IP Phones with CLS Default Virtual Office Login Allowed (DVLA). The IP Phone with CLS DVLA is considered to be inactive if no key was pressed on the IP Phone during a configured period of time.

For more information, see “Virtual Office logout during midnight routines” in *Features and Services Fundamentals, NN43001-106*.

Virtual Office logout rule on IDLE condition

This features allows an administrator to configure a rule for automatic logout of idle DVLA (Default Virtual Office Login Allowed) IP Phones. The DVLA logged-in IP Phones which are idle for a specified time can be automatically logged out. The IP Phone displays a warning message and an option to cancel the logout and reset the IDLE timer.

For more information, see “Virtual Office logout on IDLE condition” in *Features and Services Fundamentals, NN43001-106*.

Virtual Office Login/Logout for Multiple Line Appearance

This feature allows Virtual Office login/logout when there is Multiple Line Appearance of other telephones on an IP Phone when one of line keys is in use; that is, a call to a multiple-appearance DN is originated or terminated by another appearance.

Virtual Office login to a IP Phone with Multiple Line Appearance

IP Phone A with Virtual Office Login Allowed (VOLA) class of service tries to perform a Virtual Office login to IP Phone B with Virtual Office User Allowed (VOUA) class of service. IP Phone B has a multiple appearance DN configured as Single Call Ringing/Non-ringing (SCR/SCN).

Another appearance of IP Phone B’s multiple appearance DN is located on another telephone and has an active call; there is no active call on IP Phone B. In this case, Virtual Office login from IP Phone A to IP Phone B is successful if any other DN configured on IP Phone B is used for the login.

Virtual Office logout from an IP Phone with Multiple Line Appearance

IP Phone A with VOLA class of service is Virtual Office logged in to IP Phone B with VOUA class of service. IP Phone B is in a Virtual Office logout state. The Terminal Number (TN) of IP Phone B has a multiple appearance DN configured as SCR/SCN.

Another appearance of IP Phone B’s multiple appearance DN is located on another telephone and has a call at the moment; there is no active call on the TN of IP Phone B. In this case, IP Phone A successfully performs Virtual Office logout from IP Phone B and IP Phone B returns to its home TN.

Virtual Office login from an IP Phone with Multiple Line Appearance

An IP Phone with VOLA class of service has a multiple appearance DN configured as SCR/SCN. Another appearance of the same DN is located on another telephone and has a call at the moment; there is no active call on the IP Phone. In this case, the IP Phone can perform a Virtual Office login to any IP Phone with VOUA class of service.

For more information, see “Virtual Office Login/Logout for Multiple Line Appearance” in *Features and Services Fundamentals, NN43001-106*.

Support of two lines on single-line-display IP Phones for Corporate Directory, PD, RL and CL

This feature provides the following functionality for the IP Phone 1120E, IP Phone 2002, IP Phone 1220, and IP Phone 1230:

- Personal Directory/Redial List/Callers List scrolls records by DN.
- Corporate Directory switches between CARD and LIST modes.

ESA calls during Virtual Office logout state

Some IP Phones are configured as Virtual Office-only telephones and have no assigned DN. However, these IP Phones can still be used to make emergency calls. “Emergency Calls only “ is displayed on the IP Phone display when not logged in to Virtual Office. When the IP Phone goes off-hook, dial tone is available for emergency calls only. All other calls are restricted.

Administrator VO logout option

This features lets a CS 1000 administrator search for Virtual Office logged-in IP Phones, based on idle time criteria, and log them out, based on the duration for which the IP Phone is idle, or log out a particular IP Phone.

Only personnel with LD 117 permission can perform these operations.

For more information, see “Virtual Office Administrator logout” in *Features and Services Fundamentals, NN43001-106*.

Enhanced Virtual Office login messages

Standard VO login numeric messages have been updated with more descriptive messages which help to understand the error or condition.

Provisioning of four additional keys for the IP Phone 1165E

CS 1000 Release 7.0 removes the Release 6.0 limitation of 12 supported keys on the IP Phone 1165E. Previously, keys from 0 to 5 were located on the first page of the IP Phone and keys from 6 to 11 were located on the second page. In Release 7.0, the first page contains keys 0-7 and the second page contains keys 8-15.

During an upgrade from Release 6.0 to Release 7.0, the 6 and 7 keys are moved from the second page to the first page and keys 8-15 are displayed on the second page.

Call Deflect key

This feature allows a user to deflect an incoming call. If a user presses the Deflect feature key, then the incoming call is redirected with the same treatment as if the line was busy and HUNT DN was configured. If HUNT DN is not configured or HTD (Hunt DN Denied) is configured, then the call originator receives a busy signal. The Deflect key feature is intended to deflect a call to voice mail or to another DN when the user does not want to answer the call and does not want to wait until Call Forward No Answer processes the incoming call.

This feature is not applicable to IP Phones without feature keys, such as the IP Phone 2001, IP Phone 1110, and IP Audio Conference Phone 2033.

For more information, see “Call Deflect for IP Phones” in *Features and Services Fundamentals, NN43001-106*.

Single sign-on for Electronic Lock with Virtual Office

This feature provides the IP Phone user with single sign-on and authentication for both Virtual Office login and Electronic lock. The IP Phone user does not have to authenticate Virtual Office login and then authenticate Electronic Lock to make outgoing calls.

Chapter 12: Corporate Directory

The Communication Server 1000 Corporate Directory allows M3900s and IP Phones to display and access a corporate-wide telephone directory. UCM Common Services provides a Corporate Directory application that generates the corporate directory file and uploads it to CS 1000 systems.

For more information about Corporate Directory, see *Signaling Server IP Line Applications Fundamentals (NN43001-125)*

Chapter 13: Numbering Groups

A numbering group represents common numbering planning attributes which are shared by a group of subscriber telephony accounts. Each telephony account can belong to only one numbering group. If a telephony account does not belong to a specified numbering group, it is classified as a member of the default numbering group category. A member of the default numbering group category only uses a private numbering plan (private CDP and UDP dialing). The Numbering Group application is installed in UCM Common Services at the Network level under CS1000 Services.

For more information about Numbering Groups, see *Signaling Server IP Line Applications Fundamentals (NN43001-125)*.

Chapter 14: DMC DECT Manager

Nortel Integrated DECT (DECT) allows users to move freely about their work sites while conducting telephone conversations using wireless handsets. DECT is an acronym for Digital Enhanced Cordless Telecommunications.

In Communication Server 1000 Release 7.0, DMC DECT Manager is available as a stand-alone application. The DMC DECT Manager can not co-reside with Telephony Manager.

Application features

The DMC DECT Application allows you to do the following:

- view the MDECT System provisioning with the DECT Systems window
- view the DMC8 configuration with the Boards (DMC) window
- view base station configuration with the Radio Fixed Part (base station) window
- view subscription information with the Subscriptions window
- upgrade firmware using the DECT Systems window
- subscribe handsets using the Subscriptions window
- support DMC-8 and DMC (serial only)
- synchronize (update) the DECT Application database to the MDECT system configuration when the DECT Manager connects to the MDECT system
- collect performance data using the Performance Collection window

For more information about DMC DECT Application, see *Using the DMC DECT Manager , NN43001-142*.

Chapter 15: SIP Line DECT

Traditional Digital Enhanced Cordless Telecommunications (DECT) is an application on the system that allows digital wireless capabilities. With DECT, users can travel around their work sites while answering a call, making a call, continuing a call, or transferring a call.

Session Initiation Protocol (SIP) DECT on SIP Line provides the features of traditional DECT by allowing the SIP DECT system to interact with CS 1000 through the SIP Line gateway.

The following is a list of features that are available on SIP DECT on SIP Line but are not available on traditional SIP DECT, or are improvements on traditional SIP DECT features.

- Call hold
- Call transfer - Two types of call transfers are possible:
  - Blind transfer
  - Consultative transfer
- Conference

Prior to Communication Server 1000 (CS 1000) Release 7.0, it was possible to connect SIP clients using the SIPN connection method. Beginning in CS 1000 Release 7.0 the SIPN connection method is no longer supported; however, a procedure is provided to upgrade a SIPN connection to a SIPL connection.

SIP DECT on SIP Line offers Multi-Site Mobility Networking (MSMN) functionality; MSMN automatically routes calls from a primary CS 1000 to visitor CS 1000 systems to which the user may travel. Visitor sites must have a SIPL Universal Extension (UEXT) TN configured with appropriate SIP registration parameters. Both SIPN and SIPL connection methods are valid for MSMN. MSMN supports Message Waiting Indicator (MWI) status updates during registration attempts or when there is a status change.

For more information about SIP DECT on SIP Line, see *SIP DECT Fundamentals, NN43120-123*.

Chapter 16: SIP Line enhancements

Communication Server (CS) 1000 Release 7.0 brings a significant capacity increase to the SIP Line Gateway (SLG). SLG servers support a maximum of 3700 users for each SLG, which is double the number of SIP Line users (1800) in Release 6.0. Low hardware costs and fewer servers are required in large installations.

Multiple Line Appearance or Bridged Line Appearance

New Business Grade Telephony features are part of the CS 1000 Release 7.0, with key features for work group communications. A desktop user can have Multiple Line Appearances on their IP Phone 1100 and 1200 series telephones, now running SIP firmware. You can view other users' lines, share lines for group call coverage, and make or receive phone calls on various Directory Numbers (DNs) within a single IP Phone with SIP firmware. Bridged Line Appearance can join a call from a different IP Phone or place. A call on hold on one telephone can receive the call from another phone sharing the line appearance.

SIP firmware 3.2

CS 1000 Release 7.0 supports new SIP firmware Version 3.2 capabilities for SIP and IP Phones. SIP firmware 3.2 is available with Communication Server 1000 Release 7.0 and has new features for both the 1100 series (1120E, 1140E, and 1165) and 1200 series (1210, 1220, and 1230) IP Phones running SIP firmware 3.2. In addition, Release 7.0 has a new firmware management and provisioning utility for SIP IP Phones and new SIP firmware 3.2 capabilities (for example, TLS, access to key core features for SIP lines) for SIP Line users.

Chapter 17: Multiple Routes for SSG

CS 1000 Release 7.0 adds the capability to SIP Signaling Gateway (SSG) to define and configure two external facing routes, whereas for Release 6.0 you could configure only one external route. Customers can use this capability to reduce requirements for extra hardware to support a second dedicated SSG by using this multiple route capability.

For more information about Multiple Routes for SSG, see *IP Peer Networking Installation and Commissioning (NN43001-313)*.

Chapter 18: Calling Line Restriction Override

CS 1000 Release 7.0 introduces Calling Line Restriction Override feature.

Calling Line Restriction Override feature

With the Calling Line Restriction Override feature, calling party information can be unblocked on a Set and CDN basis.

When the CLS on the terminating telephone (analog CLASS or digital) is set to CROA (Calling Line Restriction override allowed), the Calling Line Identification (CLID) Presentation Indicator changes from restricted or denied to allowed. In the case of CDN, this can be done by setting CLRO prompt to YES. This is applicable to all the local and trunk calls.

For more information, see “Calling Line Restriction Override” in *Features and Services Fundamentals, NN43001-106*.

Chapter 19: Patching Manager enhancements

Overview

Patching Manager for Communication Server 1000 Release 7.0 includes the following enhancements:

- Binary patching support
- Loadware support
- Deplist support
- Linux Call Server (VxELL) patching support
- Enhanced Linux service pack support
- High Scalability support
- Enhanced color coding to indicate user actions, warnings, and errors

For more information, see *Patching Manager Fundamentals, NN43001-407*.

Binary patching support

Central Patching Manager now supports the management, activation, and deactivation of binary patches for VxWorks elements, such as Call Servers and Media Cards.

Loadware support

Central Patching Manager now supports the management, activation, and deactivation of MGC and PSDL loadware.

Deplist support

Central Patching Manager now supports the management, activation, and deactivation of deplists.

Linux Call Server (VxELL) patching support

Call Servers installed on Linux now support binary patches and deplists.

Enhanced Linux service pack support

Search Service Pack (Standard + Site-specific service pack) A site-specific service pack that contains additional patches or serviceability updates that are not part of the standard service pack.

Delta Service Pack (Target-specific service pack) A target-specific service pack is generated for a specific element.

High Scalability support

Central Patching Manager provides the ability to view VxWorks and Linux targets in a tree view. Each top-level node can be expanded to show its associated elements.

Enhanced color coding

The Patching Manager interface now displays color coded messages to indicate user actions, warnings, and errors.

Chapter 20: IP Attendant Console 3260

Overview

The IP Attendant Console 3260 is an IP-enabled Attendant Console that replaces the need for a Personal Computer Console Interface Unit (PCCIU) or M2250 Digital Attendant Console for supported third-party Attendant Console clients. A Software Development Kit (SDK) is required for enabling IP signaling and voice for third-party clients. IP Attendant functionality is included with IP Media Services, which is installed as part of Signaling Server software.

Note:
The IP Attendant Console 3260 is not supported for Communication Server 1000M systems.

The IP Attendant Gateway uses Session Initialization Protocol (SIP) to manage signaling between the IP Attendant Console and the Media Application Server (MAS). Communication with the Call Server is managed using the existing Transmission Control Protocol (TCP).

IP Attendant Consoles are configured on virtual loops. You can configure up to 63 attendant consoles (of type M2250, IP 3260, or a combination of both) on each system. You can only configure the number of consoles permitted by ISM License parameters.

Features

The IP Attendant Console 3260 has the following predefined features:

Table 2: Predefined features of the Attendant Console 3260

Mnemonic	Label
C/H	Centralized Auto-Attendant Service
B/N	Position Busy/Night Service
excl src	Exclude Source
excl dest	Exclude Destination
RLS src	Release source
RLS dest	Release destination
SHIFT	Shift key

Mnemonic	Label
HOLD	Hold
lpk 0	Loop pickup 0
lpk 1	Loop pickup 1
lpk 2	Loop pickup 2
lpk 3	Loop pickup 3
lpk 4	Loop pickup 4
lpk 5	Loop pickup 5
RLS	Release

Supported KEY (LD 12) features

The IP Attendant Console 3260 supports the following KEY (LD 12) features.

Table 3: Supported KEY (LD12) features for the IP Attendant Console 3260

Mnemonic	Description
ADL	Autodial
AWU	Automatic Wake Up
BIN	Barge-In
BKI	Break-In
BVR	Busy Verify
CHG	Charge Account
COS	Controlled Class of Service
CPN	Calling Party Number
DCW	Display Call Waiting
DDL	Do Not Disturb Individual
DPD	Display Destination
DPS	Display Source
DRC	DID Route Control
EES	End-to-End Signaling
GND	Group Do Not Disturb
MCK	Message Cancellation

Mnemonic	Description
MDT	Maintain Date/Display Date
MIK	Message Indication
MTM	Maintain/Display Time
MTR	Meter
NAS	Network Attendant Service
PRK	Call Park
RDL	Redial stored number
RFW	Attendant Remote Call Forward
RPAG	Radio Paging
RTC	Routing Controls
SCC	Speed Call Controller
SECL	Series Call
SSC	System Speed Call Controller
TRC	Malicious Call Trace

For more information about IP Attendant Console 3260, see *Features and Services Fundamentals—Book 4 of 6, NN43001-106*.

Chapter 21: SIP Media Gateway

Tertiary NRS

A tertiary NRS server for a SIP Gateway is introduced in Communication Server (CS) Release 7.0 to provide a third level of redundancy. The tertiary NRS can run on any device on the network and can operate in a one-for-many or in a one-to-one mode. The tertiary NRS server replaces the existing Failsafe operations. The tertiary NRS has a database that is independent of the primary NRS that is tailored for routing calls during a WAN outage scenario. This is different from the failsafe NRS which has a snapshot of the database on the primary NRS. The tertiary NRS can be configured from the SIP Trunk Gateway settings in Element Manager.

For more information, see *IP Peer Networking Installation and Commissioning , NN43001-313*.

On-net to off-net conversion

In CS 1000 Release 7.0, the automatic on-net to off-net overflow capability of the ESN Network Alternate Route Selection (NARS) feature is enhanced to remove the current restrictions on the provisioning of the ESN NARS data for converting a number that was dialed using Uniform Dial Plan (UDP) to the Listed Directory Number (LDN) or Direct Inward Dial (DID) number of the destination location. Off-net facilities are used to complete the call. This feature is activated on each route list entry where required. This enhancement also simplifies the provisioning for on-net to off-net conversion for customer locations outside of North America.

For more information, see *Basic Network Feature Fundamentals , NN43001-579*.

Alternate Call Routing for unregistered resources

Alternate Call Routing (ACR) has been enhanced for CS 1000 Release 7.0 to include ACR for unregistered resources. This feature reroutes calls if the terminating resource, such as a telephone or DSP, is unregistered locally but is likely to be registered elsewhere in the network. This feature can be enabled from LD 117 using the Zone Alternate Route Table (ZALT) or through Element Manager.

For more information, see *Dialing Plans Reference , NN43001-283*.

ZBD DMI

To reduce the number of Digit Manipulation Input (DMI) entries required when Survivable SIP Media Gateways (SSMG) are in several countries, the recommended dial pattern is to send the digits as E.164 international numbers. This is achieved in Release 7.0 by enhancing the DMI entry to recognize the character C for Country Code. The Country Code of the originating TN replaces the C character in the dialed digit string.

For more information, see *Dialing Plans Reference , NN43001-283*.

Chapter 22: IPv6

IPv6 is an evolution of the current IPv4 standard of today.

In Communication Server (CS) Release 7.0, global unicast address is the only type of IPv6 addressing supported. For example: 2001:DB8::214:c2ff:fe3b:3588 In this example, the symbol, :: represents a continuous sequence of zeros and appears only once in the IPv6 address. This is a compressed form to reduce the length of the IPv6 address. For example, the multicast address FFED: 0000:0000:0000:0000:BA98:3210:4562 in compressed form is FFED::BA98:3210:4562.

The migration to IPv6 is being driven by governments worldwide. The United States government has been a driving force by passing legislation to consider IPv6 compatibility in procurement decisions. With Release 7.0, the CS 1000 supports dual-stack SIP devices to offer a choice between IPv6 and IPv4.

The address type IPv6 and IPv4 supports both the IPv6 primary and secondary TLAN addresses along with IPv4 primary and secondary TLAN addresses.

The IPv6 feature is compatible with:

- SIP and SIP TLS
- RTP media stream
- Existing and new (CP DC, CP MG) hardware platforms
- Mindspeed-based media hardware (MGC daughterboards and Media Cards, incl. DSP-DB 32, 96, and 128)
- MC32S (Mindspeed-based)
- Main office / branch office operation
- High availability
- N-way geographical redundancy
- Collaborative NRSs

Functionality supported over IPv4 only:

- H.323
- IP Line Cards, IP Trunk Cards, VGMC and MC32 media cards (all Telogy-based)
- Distributed MGCs which connect to CS through the ELAN
- Communication Server 1000 SIP Trunk Bridge
- IP Media Services
- UNIStim endpoints (this may be a future development)

Chapter 23: Mobility X enhancements

Capacity Enhancement

Mobile X user database stores the mapping between mobile CLID and UEXT directory number (DN). The maximum number of entries in Mobile X user database or the Mobile X hash table has been increased from 4000 to 12000 per user in CS 1000 Release 7.0.

Cellular Voice Mail Avoidance

The cellular voice mail avoidance feature is an enhancement to the existing condition which allows the mobile user to route a call to cellular voice mail if the user’s cell phone is turned off.

Ring Again no answer/Ring Again on busy

The mobile user activates the Ring Again (RGA) feature when the call to a destination party is ringing and does not answer, or when the destination party is busy. The mobile user who activates the RGA no answer/ busy feature is notified when the destination party's call is terminated. The notification is a short call to the mobile number by the CS 1000.

Simplified UI for Mid-Call features

A simplified User Interface (UI) allows the MobileX user to use mid-call features more easily than with the traditional UI. In the simplified UI, the Mobile user in an established call can initiate the second call using Mid-Call features by dialing MFAC and the target DN.

Mobile X over SIP support – Mid call features

This enhancement allows MobileX to be supported over SIP trunks. Mid-call features are supported for MobileX calls over SIP. Simple calls, busy status, OCS presence, and call handoff are supported. If CS 1000 SIP Trunk is deployed, mid-call features are supported as media anchoring (using SIPX) on CS 1000 for VTRK tandem calls.

Dialable Single Number Mobile Number

You can use the Dialable Single Number Mobile Number (SNMN) feature to reach a Mobile User either by PBX or a cell number. Dialable SNMN is an extension of the Mobile Number Single Number feature. In the Mobile Number Single Number feature, the caller can reach a MobileX user by dialing the E.164 mobile number.

Dialable Cell CLID enhancement

The Dialable Cell Calling Line ID (CLID) feature displays the CLID of both internal and external calls originated by the MobileX user. The user can specify whether the CLID is to be displayed in geographic CLID (GEO CLID) mode or cellular CLID (CELL CLID) mode.

Chapter 24: Security enhancements

This chapter describes security enhancements introduced in Communication Server (CS) 1000 Release 7.0.

Intra System Signaling Security

Intra System Signaling Security (ISSS) provides authentication and encryption for internal signaling messages within a CS 1000 system. In Release 7.0, ISSS management has been enhanced to provide improved performance and support for large security domains. The following enhancements are new:

- Allowing ISSS management operations (Synchronize/Activate) to subsets of the security domain, specifically an individual CS 1000 system or a CS 1000 High Scalability (HS) system.
- Manual ISSS targets are associated with individual CS 1000 systems rather than all systems in the Unified Communications Management (UCM) security domain.
- Manual ISSS targets are available as elements in UCM.
- ISSS settings (PSK & level) are now specified as an ISSS policy that can be applied to individual CS 1000 systems.

Security Domain Manager

Security Domain Manager (SDM) improvements have been made in CS 1000 Release 7.0. There are additional registration commands for a Media Gateway Controller (MGC) or Media Card that are not registered to the UCM Security domain, and also registration commands for a single MGC or Media Card to the UCM security domain from the Call Server CLI.

The following commands have been updated with the newly added commands:

Release 6.0 command	Updated for Release 7.0
Join Security Domain:	
REGISTER UCMSECURITY SYSTEM	REGISTER UCMSECURITY SYSTEM FORCE
REGISTER UCMSECURITY DEVICE	REGISTER UCMSECURITY CS

Release 6.0 command	Updated for Release 7.0
Leave Security Domain:	
UNREGISTER UCMSECURITY DEVICE	UNREGISTER UCMSECURITY CS
Stat:	
STAT UCMSECURITY DEVICE	STAT UCMSECURITY INFO

UCM Search and Filter

In CS 1000 Release 7.0, the UCM interface provides a search and filter capability. You can easily perform searches to access large amounts of data. The matching results and the search criteria are stored in memory for future use. The search is performed on the data in persistent storage. The filter operation is performed to obtain matching results from the search criteria in memory.

For more information, see *Unified Communications Management Common Services Fundamentals, NN43001-116*.

UCM security server demote

CS 1000 Release 7.0 has introduced a demote operation in UCM to allow you to convert a UCM security server to a UCM member server. This is beneficial as it enables an administrator to merge multiple smaller UCM domains into a single domain without having to reinstall.

For more information, see *Unified Communications Management Common Services Fundamentals, NN43001-116*.

Chapter 25: Network Routing Service Management enhancements

Network Routing Service Management (NRSM) for Communication Server 1000 Release 7.0 includes the following enhancements:

- IPv6 support
- Different Route Cost modification
- NRS Bulk Import/Export enhancements
- Media Application Server support

IPv6 support

This feature helps to configure single stack (IPv4 only) and dual stack (both IPv4 and IPv6) in NRSM. NRSM provides support for IPV6 format for the TLAN IP address in the User Interface (UI). It also provides support for adding IPv6 endpoints. For more information about the IPv6 in NRS server, see *Network Routing Service Fundamentals (NN43001-130)*.

Different Route Cost modification

In Communication Server Release 7.0, the NRSM code is modified to display an error message if a new routing entry is added which has the same DN type and DN prefix as another routing entry that is already present under the same Gateway Endpoint. For more information about Route cost modification, see *Network Routing Service Fundamentals (NN43001-130)*.

NRS Bulk Import/Export enhancements

When importing routing entries on the system, it is mandatory that all service domains, L1 domains, L0 domains and endpoints be present in the database for a successful import of the routing entries. A predefined template or a set of data can be customized locally with a spreadsheet and imported on a system prior to installation. This enhancement in Release 7.0 extends the concept of the NRS bulk import or export to include more information to capture in the CSV file. When importing data from that CSV file, the import process supports the creation of service domains, L1 domains, L0 domains and endpoints automatically if not

present in the NRS database. For more information about NRS enhancements, see *Network Routing Service Fundamentals (NN43001-130)*.

Media Application Server support

The feature helps to configure Media Application Server (MAS) parameters for SIP endpoints in NRSM. NRSM provides support for adding the URI parameters in a SIP enabled Gateway endpoint in the User Interface. For more information about Media Application Server, see *Network Routing Service Fundamentals (NN43001-130)*.

Chapter 26: Call Alert

The Call Alert feature provides an audible indication of an incoming call to all members of a Ringing Number Pickup Group (RNPG) by providing a single buzz tone after the time specified in the Directory Number Delayed Ringing (DNDR) prompt, as well as a visual indication.

For example: two CS 1000 users, User A and User B are configured in the same RNPG group and with the appropriate class of service to allow call pickup. User C is another user in the same CS 1000 system and does not belong to the same group. If C calls A, then A will see the name and number of C on the display; B will see the name and number of A on the first line and the name and number of C on the second line of the display. If A has not answered the call after the time configured in DNDR, B hears a short buzz.

The telephones must have CLS PUA (Pickup Allowed) configured. In LD 15, the Call Alert feature introduces the new response GPAA/GPAD (Group Pickup Alert Allowed/Denied) for the OPT prompt. RNPG and DNDR are configured in the usual manner in LD11.

For more information, see “Call Alert” in *Features and Services – Book 2 (NN43001-106-B2)*.

Chapter 27: Bandwidth Management zone enhancements

In Communication Server (CS) 1000 Release 7.0, the range of allowable Bandwidth Management (BWM) zone numbers is increased from 0-255 to 0-8000.

Element Manager configuration of BWM zones retains the basic functions of add, edit, import, export, and delete. In CS 1000 Release 7.0, Element Manager uses a new sortable table to display bandwidth zones and their basic properties.

Prior to Release 7.0, bulk import of bandwidth zone values was supported using an Excel file. In Release 7.0, bulk import supports a CSV file format.

Caution:

Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release, you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.

Chapter 28: MAS deployment

The Media Application Server (MAS) is a software platform for hosting multimedia applications. Communication Server 1000 Release 7.0 introduces the MAS software platform installed and configured on a Commercial Off The Shelf (COTS) 2 or Common Processor Dual Core (CP DC) server.

MAS deployment

MAS is deployed as a standalone application on a COTS 2 or CP DC server. MAS software is deployed using the Deployment Manager; the MAS software load is uploaded to the Deployment Manager Library, which deploys the software to target servers in the security domain. You can preconfigure (stage) deployment targets to logically configure the member and backup servers before physically installing the Servers and joining them to the domain. During preconfiguration, you allocate the servers into the hierarchical groups which determines the application packages required for deployment. If you intend to deploy MAS to a server, you allocate that server to the Network Services group.

Note:

The MAS software load is contained in a .nai file that has the following format: nortel-cs1000-linux-mas-700xx-pyyy-mzz.nai

For more information about adding a software load or deploying MAS software to a COTS 2 or CP DC server, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Hardware platforms

You can deploy MAS on the following hardware platforms:

- CP DC card
- Dell R300
- IBM x3350

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

Chapter 29: Software Input/Output prompts, responses and commands

Overview

The information in this chapter outlines the new, changed, or retired information in the Software Input/Output Reference documents (NN43001-611 and NN43001-711) for Communication Server 1000 Release 7.0.

LD 11: Digital Telephone Administration

The following prompts and responses are added to LD 11.

Table 4: LD 11: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
MRT	xxx	Music route number. The route type can be MUS or IMUS. The default is none.	basic-7.00
CLS	DVLA	Default Virtual Office Logout Allowed	basic-7.00
	DVLD	Default Virtual Office Logout Denied (default) **Note:** An IP Phone is in Virtual Office logout state by default. Can only be used for Virtual Office login.	basic-7.00
	MUTA	Mute key functionality allowed on IP Phone (default)	basic-7.00
	MUTD	Mute key functionality denied on IP Phone **Note:** MUTA and MUTD are applicable only to IP phones with a Mute key	basic-7.00
	MWTA	Message Waiting Tone allowed	basic-7.00

Command	Response	Description	Pack/Rel
	MWTD	MWTD: Message Waiting Tone denied (default) **Note:** MWTA and MWTD are applicable for IP Phones only.	basic-7.00
	SBMA	Set-based Music on Hold Allowed	basic-7.00
	SBMD	Set-based Music on Hold Denied	basic-7.00
	RECA	Call Recording allowed	pkg-411
	(RECD)	Call Recording denied	pkg-411

LD 12: Attendant Consoles

The following prompts and responses are added to LD 12.

Table 5: LD 12: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
ZONE	0-255	Zone of the IP Attendant	basic-7.00
IPCR	(NO)/YES	Allow IP Call Recording	basic-7.00
TYPE	3260	IP Attendant Console 3260	basic-7.00

LD 14: Trunk Data Block

The following responses are added to LD 14.

Table 6: LD 14: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
TYPE	IMUS	IP Music trunk	basic-7.00
	IRAN	IP Recorded Announcements trunk	basic-7.00
XTRK	IPMS	IP Media Services extended trunk	basic-7.00

LD 15: Trunk Data Block

The following prompt is added to LD 15.

Table 7: LD 15: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
MSRN	x…x	Media Services Routing Number	basic-7.00
FOPT	0-(6)-30	The number of seconds in two second intervals that CFW (Call Forward) or ACR (Alternate Call Routing) should be suspended on a phone that has just forwarded or routed a call off-node. Odd entries are rounded up to the next valid entry. A response of 0 disables FOPT.	basic-7.00

LD 16: Route Data Block, Automatic Trunk Maintenance

The following prompts and responses are added to LD 16.

Table 8: LD 16: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
ZONE	0-255	Zone for codec selection and bandwidth management	basic-7.00
NODE	xxxx	Node ID	basic-7.00
RTYPE	MAS	Media Application Server. Chosen automatically for IRAN RDB type	basic-7.00
TYPE	IMUS	IP Music route data block	basic-7.00
TKTP	IRAN	IP RAN route trunk type	basic-7.00

LD 17: Configuration Record 1

The following prompts are added to LD 17.

Table 9: LD 17: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
IPCONF	0-255	Virtual IP conference loop. Precede a loop number with X to remove it. You can remove multiple loops at the same time. **Note:** Before a loop can be removed, it must first be disabled.	basic-7.00
__NODE	1-9999	Node ID of the IP Ad Hoc Conference loop	basic-7.00
IPTONE	0-255	Virtual IP tone loopk	basic-7.00

LD 20: Print Routine 1

The following response is added to LD 20.

Table 10: LD 20: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
TYPE	ASTS	Associate (AST) Sets	basic-7.00

LD 26: Print Routine 1

The following response is added to LD 20.

Table 11: LD 20: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
ABR	YES (NO)	ACD Busy Routing	pkg-411
	(NO)	The agent is not presented with ACD calls when busy with an IDN call.	
	YES	The agent is presented with ACD calls when busy with an IDN call.	

LD 60: Digital Trunk Interface and Primary Rate Interface Diagnostic

The following prompts and responses are added to LD 60.

Table 12: LD 60: Alphabetical list of new prompts and response

Command	Description	Pack/Rel
VER (loop)	Query existing UDT card firmware version.	basic-7.00

LD 86: Electronic Switched Network 1

The following prompts and responses are added to LD 86:

Table 13: LD 86: Alphabetical list of new prompts and response

Command	Response	Description	Pack/Rel
RLNO	0-15	Rule number in CMDB block	basic-7.00
RNPI	a...a	Replacement Numbering Plan Indicator (a...a = E164, PRIV, E163, TELE, X121, NATL, NCHG)	basic-7.00
RTON	a...a	Replacement Type of Number (a...a = UKWN, INTL, NATL, SPN, LOCL, ELOC, CDP, CSS7, NCHG)	basic-7.00
TBNO	xxx	CLID manipulation Index numbers (1-256) in CMDB block	basic-7.00
MXCM	xxx	Maximum number of CLID manipulation lists (1-256) If MXCM = 0, the system do not allow the creation of any CLID manipulation lists.	basic-7.00
CONA	(NO) YES	Continuation Allowed to attempt the next entry of the Route List Block if local termination fails for a NARS call. Prompted when LTER=YES This operation cannot be used for Trunk Steering Code (TSC) or Distant Steering Code (DSC) configuration.	basic-7.00
CTBL	(0)-256	CLID manipulation index	basic-7.00
PROU	(1) 2	Preferred Routing. The default value is 1.	basic-7.00

Command	Response	Description	Pack/Rel
FEAT	CMDB	Feature = CMDB (flexible CLID manipulation data block)	basic-7.00
INST	X...X	Insert up to 8 leading digits in case of CMDB	basic-7.00
INST	#...#	Insert alphanumeric characters. Where #...# is: an alphanumeric string of up to 31 characters. Allowed characters are: • c = country code • p = numbering zone prefix • x = precede with x to delete previously defined value	basic-7.00

LD 117: Ethernet and Alarm Management

The following commands are added to LD 117:

Table 14: LD 117: Alphabetical list of new commands for LD 117

Command	Description	Pack/Rel
enl dvla midnlogout nnnn	Enable Automatic DVLA IP Phones Logout during Midnight Routine. DVLA IP Phone will be logged-out if it is inactive more then nnnn minutes, where: nnnn = 1- (30) - 1440 minutes	basic-7.00
dis dvla midnunreg	Disable Automatic DVLA IP Phones Logout during Midnight Routine	basic-7.00
prt dvla midnunreg	Print status of DVLA IP Phones during Midnight Routine	basic-7.00
enl dvla idlelogout nnnn	Automatic Idle DVLA IP Phones Logout is enabled A DVLA IP Phone will be logged-out if it is inactive more then nnnn minutes nnnn = 1- (30) - 1440 minutes	basic-7.00
dis dvla idlelogout	Automatic Idle DVLA IP Phones Logout is disabled.	basic-7.00
prt dvla idlelogout	Print status of Automatic Idle DVLA IP Phones Logout	basic-7.00
DVLA LOGOUTALL [<idle time>]	Logs out all DVLA logged-in idle IP Phones which are idle for more than idleTime minutes (if specified).	basic-7.00

Command	Description	Pack/Rel
DVLA LOGOUTTN <loop><shelf><card> <unit>	Logs out a specific DVLA IP Phone if it is logged in and idle.	basic-7.00
DVLA LOGOUTLIST <filename>	Parses the specified file from /e/temp/ directory on Call Server and logs out all DVLA IP Phones whose TNs are presented in the file. File must contain only the TN in string format (for example, 096 0 00 30) on each line.	basic-7.00
STIP DVLA [<idle time>]	Outputs information (TN, Prime DN, idle time) about logged-in DVLA IP Phones which are idle for more than idleTime minutes (if specified). Not more than 1000 records can be outputted at once. If more than 1000 records are collected, then Info message SCH2376 is printed.	basic-7.00
NEW ZONE <zonenumber> [<intraZoneBandwidth><intraZoneStrategy> <interZoneBandwidth><interZoneStrategy> <zoneIntent> <zoneResourceType>	Configure a new zone, where: • zoneNumber = 0–255 • Zone = 0–8000 **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255. • intraZoneBandwidth = 0-.1Mbps • intraZoneStrategy = intrazone preferred strategy, where: - BQ = Best Quality - BB = Best Bandwidth • interZoneBandwidth = 0-.1Mbps • interZoneStrategy = interzone preferred strategy, where: - BQ = Best Quality - BB = Best Bandwidth • zoneIntent = type of zone, where: - MO = Main Office zone - BMG = Branch Media Gateway zone	zcac-4.50 zcac-7.00

Command	Description	Pack/Rel
	- VTRK = Virtual Trunk zone • zoneResourceType = resource Intrazone preferred strategy, where: - (shared) = shared DSP channels - private = private DSP channels	
NEW RANGE_OF_ZONES <zoneStartNumber> <zoneAmount> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType>	Create new bandwidth zones. This command creates a range of new bandwidth zones starting from <zoneStartNumber>. The number of existing bandwidth zones must be less than 8001. If the number of existing bandwidth zones is greater than or equal to 8001, no bandwidth zones are created.	basic-7.00
OUT RANGE_OF_ZONES <zoneStartNumber> <zoneAmount>	Remove a range of existing bandwidth zones. This command deletes a range of existing bandwidth zones, starting from <zoneStartNumber>. If there are no bandwidth zones with a zone number greater than <zoneStartNumber>, then no bandwidth zones are deleted.	basic-7.00
GEN ZONEFILE <filename>	Generate a CSV file that contains information for all configured zones on the Call Server.	basic-7.00
IMPORT ZONEFILE <filename>	Read a CSV file and create new zones listed in the file, or apply updates contained in the CSV file for zones that already exist.	basic-7.00
PRT INTERZONE	Print interzone statistics for the range between the near and far zones.	basic-7.00
PRT INTRAZONE	Print intrazone statistics for all zones or for the specified zone.	basic-7.00
STAT SERV APP <applicationType>	Display the link information status of the server for the specified application. Where <applicationType> is:	basic-7.00

Command	Description	Pack/Rel
	• IPCONF: Prints only the status of servers that have IP Ad Hoc Conference listed as an application. • IPMUS: Prints only the status of servers that have IP Music listed as an application. • IPATTN: Prints only the status of servers that have IP Attendant listed as an application. • IPTONE: Prints only the status of servers that have IP Tone listed as an application.	
STAT SERV TYPE <3260>	Print IP Attendant Console 3260 status.	basic-7.00
CHG ZSRN <Zone> <CustomerNo>	Add or change a MSRN.	basic-7.00
OUT ZSRN <Zone> <CustomerNo>	Remove a MSRN. The zone number must be specified. The customer number is optional. If no customer number is entered, all MSRNs for that zone are removed.	basic-7.00
PRT ZSRN <Zone> <CustomerNo>	Print a MSRN. Add the zone and customer number to print the MSRN for a specific zone or customer. Leave these values blank to print all MSRNs.	basic-7.00
PRT CSRN <CustomerNo>	Print the MSRN by customer number. This command prints all zones and routing information for the specified customer.	basic-7.00

LD 143: Customer Configuration Backup and Restore

The following response is added to LD 143.

Table 15: LD 143: Alphabetical list of new prompts and response

Command	Description	Pack/Rel
UPGUDT l s c	Perform UDT card firmware upgrade	basic-7.00
UPGUDTABORT	Abort UDT card firmware upgrade	basic-7.00
UPGUDT STAT	Query current UDT card firmware upgrade status	basic-7.00

Software Streamlining

The software streamlining development simplifies the administration of Communication Server 1000 by removing prompts and responses that are no longer valid. This reduces complexity, and the time spent in administering the system. Software streamlining should improve the real-time performance of the system.

The information in the following sections summarizes the software packages that are no longer available, and the prompts and responses that are no longer valid for Communication Server 1000 Release 7.0. All features, components or cards using these software packages, or using these prompts and responses should be replaced prior to upgrading to Communication Server 1000 Release 7.0.

Hardware support removed by this development includes all existing Peripheral Equipment loops and cards, including single, double and quad density terminal loops, the corresponding 1.5Mb/s and 2.0Mb/s Remote Peripheral Equipment loops, and the EPE line cards that are applicable only to those loops. Standalone TDS, MFS and Conference loops are also removed from the system. Customers with CS 1000M systems must migrate all tone and conference loops to XCT cards.

Software Packages

The following software packages, most previously discontinued, are now completely removed from the software.

Table 16: Software packages that are no longer available

Description	Package number
2.0Mb/s Remote Peripheral Equipment	165
Automated Modem Pooling	78
CDR Link	6
Command and Status Link for Alpha Terminals	85
Communications Management Accounting Center	30
Digit Key Signaling	180
Mobility Software	302, 303, and 314
Multiple Languages	264-280
Remote Peripheral Equipment	15
TDET	65

Description	Package number
Universal Wireless Interactive Networking	345
VMBA	246

LD 10: Analog (500/2500) Telephone Administration

The following prompts and responses are no longer valid.

Table 17: LD 10: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
TN	c u	Format for Small System, where: c u = card, unit • c = 1-50 • u = 0-15	basic-16
	c u	Format for CS 1000S, where: c u = card, unit • c = 11-14, 17-24, 27-34, 37- 44, 47-50 • u = 0-31	basic-1.0
	c u	Format for MG 1000B Chassis, where: c = card and u = unit • c = 0-4, 7-10 • u = 0-31 Format for MG 1000B Cabinet, where: c = card and u = unit • c = 0-10 • u = 0-31 **Note:** For converted Small Systems only, the Meridian Mail card must be installed in slot 10 if Meridian Mail is to be supported.	basic-4.00
	c u	Format for MG 1000T, where: c = card and u = unit • c = 0-4, 7-10, 11-14, 17-24, 27-34, 37- 44, 47-50 • u = 0-31	basic-4.00

Prompt	Response	Description	Pack/Rel
TOTN	c u	Format for Small System, where: c u = card, unit TOTN is not prompted for Small System Model sets.	basic-16
	c u	Format for CS 1000S, where: c u = card, unit	basic-1.0
	c u	Format for MG 1000B, and MG 1000T, where: c = card and u = unit To Terminal Number. Prompted when REQ = MOV.	basic-4.00

LD 11: Digital Telephone Administration

The following prompts and responses are no longer valid.

Table 18: LD 11: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
CFTN	c u	c u = card, unit	
	c u	Small System	
	c u	CS 1000S	basic-1
	c u	MG 1000B, and MG 1000T Use this TN as a template for new sets. ACD supervisory sets cannot be copied. Associate set (AST) assignments are not copied to the new sets. With the introduction of Phantom TNs, the system checks to be sure that TNs are not moved or copied from phantom TNs to non-Phantom TNs or visa versa. CFTN appears if REQ = CPY.	basic-4.00
CLS	(CMSD)	Command and Status link Denied	csl-8
	CMSA	Command and Status link Allowed CMSA is not supported by M2317, and M3000.	
	DSI	Data Service access or IS Server TN Allowed CLS is automatically set to DTA.	
	(DSX)	Data Service access or IS Server TN Denied	cls-8
	(LVXD)	LOGIVOX Class of Service Denied	supp-10
	LVXA	LOGIVOX Class of Service Allowed	
	(ONDD)	One Number Delivery Denied for a portable	basic-22
	ONDA	Outgoing Line Preference Allowed	

Prompt	Response	Description	Pack/Rel
	(VMD)	Server Voice Messaging Denied	cls-8
	VMA	Server Voice Messaging Allowed	
KEY	HLD	Hold	supp-10
	VUP	Volume Up key (must be assigned if Volume Down is assigned)	
	VDN	Volume Down key (must be assigned if Volume Up is assigned)	
KLS	1-7	Number of Key/Lamp Strips	
TYPE	I2001	IP Phone 2001	basic-4.00
	I2002	IP Phone 2002	basic-2.0
	I2004	IP Phone 2004	basic-2.5
	I2050	IP Software Phone 2050	basic-2.0
	MPORTBL	Mobility Portable	
TN	c u	Format for Small System, where c u = card, unit • c = 1-50 • u = 0-31	basic-16
	c u	Format for CS 1000S, where c u = card, unit • c = 11-14, 17-24, 27-34, 37- 44, 47-50 • u = 0-31	basic-1
	c u	Format for MG 1000B Chassis, where: c = card and u = unit • c = 0-4, 7-10 • u = 0-31 Format for MG 1000B Cabinet, where: c = card and u = unit • c = 0-10 • u = 0-31 **Note:** For converted Small Systems only, the Meridian Mail card must be installed in slot 10 if Meridian Mail is to be supported.	basic-4.00
	c u	Format for MG 1000T, where:	basic-4.00

Prompt	Response	Description	Pack/Rel
		• c = 0-4, 7-10, 11-14, 17-24, 27-34, 37- 44, 47-50 • u = 0-31	

LD 12: Attendant Consoles

The following prompts and responses are no longer valid.

Table 19: LD 12: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
ALPD	(NO) YES	Alphanumeric Display	
CFTN	c u	For Small System	basic-16
	c u	For CS 1000S, MG 1000B, MG 1000T	basic-4.00
	c u	Format for MG 1000B, and MG 1000T, where: c = card and u = unit To Terminal Number. Prompted when REQ = MOV.	basic-4.00
DLEN	xx	Display Length (aa = (8) or 16)	
SETN	c u	Small System and CS 1000S format SETN must have same loop, shelf and card as the primary TN if TYPE = 2250. This cannot be a phantom loop.	basic-16
TN	c u	For Small System: c u = card, unit • c = 1 - 50 • u = 0 - 15	basic-16

LD 13: Digitone Receivers,Tone Detectors, Multifrequency Senders and Receivers

The following prompts and responses are no longer valid.

Table 20: LD 13: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
TYPE	DTD	Dial Tone Detector data block	
	TDET	Tone Detector data block (Not supported on Small System)	
TN	c u	For Small System: c u = card, unit The range values are: • c = 1-50 • u = 0-7 • u = 8-11 when TYPE = MFR, MFC, MFE, MFK5, MFK6 for Card 0 **Note:** Units 0-7 must be of one type. Units 8-15 must also be of one type. The new MFC/ MFE/MFK5/MFK6 units on Card 0 must be enabled using the ENLX 0 command in LD 34.	

LD 14: Trunk Data Block

The following prompts and responses are no longer valid.

Table 21: LD 14: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
MTN	l s c u	Modem Terminal Number	
TYPE	ADM	Add-on Data Module data block	basic-1
	xxx M	Small System and CS 1000S Model	
TN	c u	Terminal Number, Small System format For Option 11C • c = 1-50 • u = 0-31 For Option 11C Chassis • c = 0-4, 7-14, 17-24, 27-34, 37- 44, 47-50 • u = 0-31	basic-14
	c u	Terminal Number, CS 1000S system format	basic-1

Prompt	Response	Description	Pack/Rel
		• c = 11-14, 17-24, 27-34, 37- 44, 47-50 • u = 0-31	
	c u	Format for MG 1000B Chassis, where: c = card and u = unit • c = 0-4, 7-10 • u = 0-31 Format for MG 1000T, where: • c = 0-4, 7-10, 11-14, 17-24, 27-34, 37- 44, 47-50 • u = 0-31	basic-4.00
	c u	Terminal Number of the first Virtual Trunk. For CS 1000S system, where: c = 61-99	basic-2.0
	c u	For MG 1000T, where: c = 61-69	basic-4.00

LD 15: Customer Data Block

The following prompts and responses are no longer valid.

Table 22: LD 15: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
Data Block FTR ADCP	xxxx	All-Digital Connection Prefix	
Data Block FTR OPT	(SBD)	Flexible Incoming Tones Denied for SL-1 telephones	ftc-14
	SBA	Flexible Incoming Tones Allowed for SL-1 telephones Only with Flexible Tones and Cadences (FTC) package 125.	
TN1	c u	For Small Systems and CS 1000S	basic-3.0
TN2	c u	For Small Systems and CS 1000S	basic-3.0
TN3	c u	For Small Systems and CS 1000S	basic-3.0
TN4	c u	For Small Systems and CS 1000S	basic-3.0

Prompt	Response	Description	Pack/Rel
TN5	c u	For Small Systems and CS 1000S	basic-3.0
TN6	c u	For Small Systems and CS 1000S	basic-3.0

LD 16: Route Data Block, Automatic Trunk Maintenance

The following prompts and responses are no longer valid.

Table 23: LD 16: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
ADCP	(NO) YES	All-Digital Connection Prefix	
DTYP	aaa	Inbound/Outbound Data Port (aaa = (IOP), IDP, or ODP)	
IAMP	0-127	Inbound Modem Pool route number	
MDMP	(NO) YES	Modem Data Module Pair	
- MRAT	5-30	Modem Ring Again Timer	
OAMP	0-127	Outbound Modem Pool route number	
TYPE	ATM	Automatic Trunk Maintenance data block.	atm-19
	SCH	ATM Schedule block. Requires Automatic Trunk Maintenance (ATM) package 84.	

LD 17: Configuration Record 1

The following prompts and responses are no longer valid.

Table 24: LD 17: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
- CMS	0-15	ESDI port number used for the CSL	
- - SECU	(NO) YES	Security for Meridian Link applications	
- - INTL	1-12	Interval	
- - MCNT	10-9999	Message Count Threshold	
- - CONF	aaa	CSL Configuration (aaa = DIR or IND)	

Prompt	Response	Description	Pack/Rel
- - SATN	ls c u	SADM/Data Line Card TN	
- - IDLP	0-254	IND DTI Loop	
- CONF	a...a	Conference loop	
- DLOP	lll dd ff	Digital Trunk Interface Loop or Loops (lll = loop number 0 - 255, dd = number of voice or data calls, ff = frame format)	basic-7
- - IDLP	0-254	DTI loop number used for IND CSL loop	
- MFSD	0, 2, 4...255	Multifrequency Sender loop	
- MPED	(SD)	Single (Maximum Peripheral Equipment Density)	
	DD	Double (Maximum Peripheral Equipment Density)	
	4D	Quadruple (Maximum Peripheral Equipment Density)	
	8D	Octal (Maximum Peripheral Equipment Density) Set to 8D for superloops. See LD 97. For Small System, MPED = 8D in the default data and must remain at this value for the peripherals to work.	
- PFTR	YES NO	Prioritize Fast Transfer feature enabled or disabled	
- REMD	a...a	Double Density Remote Peripheral Equipment loop or loops	
- REMO		Single Density Remote Peripheral Equipment loop(s)	basic-1
	0, 1, 2, ...159	Meridian 1 loop or loops	
	G0,G1...G159	GEC loop or loops	
	T0,T1...T159	TVT loop or loops Precede loop number with X to remove. If entry is for an odd-numbered loop, the preceding even numbered loop cannot be TDS, CONF or MFSD	
	0-255	Systems with Fibre Network Fabric	fnf-25
- REMQ	a...a	Quadruple density Remote Peripheral Equipment loop or loops	
- RPEB	16-1000	Remote Peripheral Equipment Buffers, 2.0 Mb/s RPE	

Prompt	Response	Description	Pack/Rel
- - SATN	ls c u	SADM/Data Line Card TN	
- SL1B	16-2048	SL-1 Buffers	
- SMEM	(NO) YES	Short Memory test	
- TDS	a...a	Tone and Digit Switch	
- TERD	a...a	Double Density Terminal equipment loop or loop	
- TERM	a...a	Single Density Terminal equipment loop or loops	
TN	c u	Valid Terminal Number, Small System Prompted when DTDT = EXT.	basic-1
- TERQ	a...a	Quadruple Density Terminal equipment loop or loops	
TRLL	1-31 1-31	Test RPE Local Loop back	rpe2-15
- USER	CDL	CDR Data Link	
- VXCT	lll	Virtual XCT loop number	

LD 21: Print Routine 2

The following prompts and responses are no longer valid.

Table 25: LD 21: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
HOUR	0-23	All routes tested by ATM for this hour	atm-7
	<CR>	Print routes tested by ATM for all hours	
TYPE	ATM	Automatic Trunk Maintenance (ATM) data block	atm-19
	SCH	Schedule data block for ATM	

LD 22: Print Routine 3

The following prompts and responses are no longer valid.

Table 26: LD 22: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
TN	c u	Print data of the specified TYPE for this card and unit (Small System).	basic-1

LD 27: ISDN Basic Rate Interface (BRI) Administration

The following prompts and responses are no longer valid.

Table 27: LD 27: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
APPL	MOB	Mobility Routing Application	

LD 30: Network and Signaling Diagnostic

The following commands and parameters are no longer valid.

Table 28: LD 30: Alphabetical list of commands and parameters that are no longer valid

Command	Parameter	Description	Pack/Rel
TTSM	loop x y z	Test Time Switch Memory (TSM) of a loop.	basic-1
TTWI	A B X Y	Test the Time Switch Memory (TSM) of the network card from B to A when timeslot Y of junctor X becomes available	fnf-25
	loop x y z	Test TSM when the timeslot junctors are idle.	basic-1

LD 32: Network and Peripheral Equipment Diagnostic

The following commands and parameters are no longer valid.

Table 29: LD 32: Alphabetical list of commands and parameters that are no longer valid

Command	Parameter	Description	Pack/Rel
DISN	l	Disable network card containing specified loop, where "loop" is the number of the even or odd loop. Not applicable to superloops.	
ENLN	l	Enable network card with specified loop, where loop is the even or odd numbered loop on the network card. Not applicable to superloops.	
SDLC	l s c	Get status of specified ISDLC card.	basic-7

LD 33: Peripheral Equipment Diagnostic for 1.5 Mb/s RPE and Fiber Remote IPE

The following commands and parameters are no longer valid.

Table 30: LD 33: Alphabetical list of commands and parameters that are no longer valid

Command	Parameter	Description	Pack/Rel
CDSP		Clears the maintenance display on active CPU to 00 or blank.	rpe-1
CMIN	ALL	Clears minor alarm for all customers	rpe-1
DISC	loop c	Disable carrier c on RPE loop. Any active calls using this carrier will be disconnected, where: loop = 0-255, System with Fibre Network Fabric	rpe-1 fnf-25
DISI	loop c	Disable carrier c on RPE loop when idle, where: loop = 0-255, System with Fibre Network Fabric Disables the carrier as soon as it has become idle. The number of channels still busy on the carrier may be checked using the STAT command. The message RPD018 indicates that the disable operation is complete.	rpe-1 fnf-25
DISL	loop	Disable specified RPE loop. Any active calls on the loop are disconnected and line transfer occurs at the remote end.	rpe-1
DISM	loop	Disable carrier status monitoring on RPE loop. Carrier failures are not detected while	rpe-1

Command	Parameter	Description	Pack/Rel
		this command is in effect. The command is canceled by the ENLM or ENLL commands.	
END		Abort current command. If no command is in progress, the active DISI command (if any) is canceled.	rpe-1
ENLC	loop c	Enable carrier c on RPE loop. If the operation is successful, OK is output. Where: loop = 0-255, System with Fibre Network Fabric	rpe-1 fnf-25
ENLL	loop	Enable RPE loop. Implies ENLM also. If the operation is successful, OK is output. If the loop is already enabled, RPD007 is output.	rpe-1
ENLM	loop	Enable carrier status monitoring on RPE loop. Where: loop = 0-255, System with Fibre Network Fabric	rpe-1 fnf-25
LDIS	loop c	List all speech channels that failed continuity test on RPE loop, carrier c. If no channels failed, response is NONE. The response is based on the results of the most recent tests (via the LOOP command) of the carrier. Where: loop = 0-255, System with Fibre Network Fabric	rpe-1 fnf-25
LOOP	loop	Perform various tests on RPE loop.	rpe-1
LRPE		List all equipped RPE loops. If no RPE loops exist, the response is `NONE` .	rpe-1
NCAR	loop	Get number of "carrier status change" messages for RPE loop.	rpe-1
SCAR	loop	Switch primary carrier on RPE loop.	rpe-1
STAT		Get number of busy channels on specified carrier in the active DISI request. If no DISI request is active, error code RPD022 is output.	rpe-1
	loop	Get status of RPE loop.	rpe-1
	loop ALL	Get status of the RPE loop, carriers and RPS card.	rpe-1
	loop c	Give status of carrier c on RPE loop.	rpe-1
	loop RPS x	Get status of RPS card x on specified RPE loop.	rpe-1

LD 37: Input/Output Diagnostic

The following commands and parameters are no longer valid.

Table 31: LD 37: Alphabetical list of commands and parameters that are no longer valid

Command	Parameter	Description	Pack/Rel
ENL	MSI x	Enable Mass Storage Interface card x.	basic-1
STAT	LINK	Provide status of all CDR links.	basic-1
	MSI	Provide status of all MSI cards.	basic-1

LD 50: Call Park and Modular Telephone Relocation

The following prompts and responses are no longer valid.

Table 32: LD 50: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
TN	c u	Old Terminal Number of set in relocation table (Option 11C format)	arie-18

LD 77: Manual Print

The following commands and parameters are no longer valid.

Table 33: LD 77: Alphabetical list of commands and parameters that are no longer valid

Command	Parameter	Description	Pack/Rel
DENL	loop	Get the density of loop.	basic-1

LD 84, 85: Set Designation Entry (ODAS)

The following prompts and responses are no longer valid.

Table 34: LD 84, 85:: Alphabetical list of prompts and responses that are no longer valid

Prompt	Response	Description	Pack/Rel
TN	c u	Small System	basic-1

Communication Server 1000 High Scalability System Common Data

Communication Server1000 High Scalability System (HS System) common data is a group of identically configured data blocks across multiple Communication Server1000E High Availability Groups (HA Groups) within the same HS System. Data that are common across multiple HA Groups are configured once and automatically propagated to all groups within the same HS System, so that the HS System appears as a single entity from a common data management perspective. For more information on HS System common data, see *Communication Server 1000E High Scalability Installation and Commissioning, NN43041-312* .

With the exception of the following prompts

- the SPVC prompt in the ATT_DATA block of LD 15
- the ALDN and PREO prompts in the FTR_DATA block of LD 15
- the VNR prompt in the NET_DATA block of LD 15

all prompts in the data blocks listed in Table 35: Default definition of common data on page 126 are included in the default definition of common data.

Table 35: Default definition of common data

Load Number	Data Block Type	Description
14	IPTI	IP TIE trunk data block
15	CDB	Customer data block
15	DEFAULT	Default customer data block
15	AML_DATA	Application Module Link options
15	ANI_DATA	Automatic Number Identification numbers
15	ATT_DATA	Attendant Console options (Except prompt SPVC)
15	CAS_DATA	Centralized Attendant Service options
15	CCS_DATA	Controlled Class of Service options
15	CDR_DATA	CDR and Charge Account options
15	FCR_DATA	New Flexible Code Restriction options

Load Number	Data Block Type	Description
15	FFC_DATA	Flexible Feature Code options
15	FTR_DATA	Features and options (Except prompts ALDN and PREO)
15	INT_DATA	Intercept treatment options
15	LDN_DATA	Departmental Listed Directory Numbers
15	MPO_DATA	Multi-Party Options
15	NET_DATA	ISDN and ESN Networking options (Except prompt VNR)
15	PWD_DATA	Customer related Passwords
15	RDR_DATA	Call Redirection
15	ROA_DATA	Recorded Overflow Announcement options
16	RDB	Route data block and Meridian 911
16	AWR	Automatic Wake Up trunk block for RAN/Music
16	CAA	Common Control Switching Arrangement
16	CAM	Central Automatic Message Accounting trunk
16	CBCT	Call by call master route cbc_pkg-23
16	COT	Central Office Trunk data block
16	CSA	Common Control Switching Arrangement access
16	DIC	Dictation trunk data block basic-1
16	DID	Direct Inward Dialing trunk data block
16	FEX	Foreign Exchange trunk data block basic-1
16	FGDT	Feature Group D trunk fgd-17
16	IDA	Integrated Digital Access
16	ISA	Integrated Service Access route or Call-by-Call
16	MCU	Meridian Communications Unit port basic-18
16	MUS	Music trunk data block
16	PAG	Paging trunk data block basic-1
16	R232	DAC for NT7D16 on RS-232 port basic-18
16	R422	DAC for NT7D16 on RS-422 port basic-18
16	RAN	Recorded Announcement trunk data block
16	RCD	Emergency Recorder trunk data block

Load Number	Data Block Type	Description
16	RLM	Release Link Main trunk data block
16	RLR	Release Link Remote trunk data block
16	TIE	TIE trunk data block
16	TIE ATL	TIE ATL data block for Sweden supp-15
16	TIE SEMI	Semi-automatic TIE trunk data block opcb-14
16	TIE AUTO	Automatic TIE trunk data block opcb-14
16	TIE TONE	Tone TIE trunk data block opcb-14
16	WAT	Wide Area Telephone Service trunk data block basic-18
17	ADAN	All input/output devices (includes D-channels) basic-19
17	CEQU	Common Equipment parameters basic-19
17	PARM	System Parameters basic-19
17	VAS	Value Added Server
24	ESA	Emergency Services Access data block
86	DGT	Digit manipulation data block
86	ESN	ESN data block
86	ITGE	Incoming Trunk Group Exclusion data block
86	RLB	Route List data Block
87	FCAS	Free Calling Area Screening
87	FSNS	Free Special Number Screening
87	NCTL	Network Control
90	NET	Network translation tables
90	HNPA	Home NPA translation code
90	LOC	ESN Location Code translation data block
90	NPA	Numbering Plan Area code translation data block
90	NSCL	Network Speed Call List data block
90	NXX	Central Office Code Translation data block
90	SPN	Special code translation data block
117	ERL	Emergency response location

Load Number	Data Block Type	Description
117	NumZone	Numbering Zone

Chapter 30: System messages

The following system messages are introduced for Communication Server 1000 Release 7.0. The new system messages are sorted by the following message categories:

The following information is available for each system message:

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

AUD: Software Audit (LD 44)

Message	Description	Action	Severity	Monitor	SNMP
AUD0128	Audit number of active music connection (MUS_AUD_ACT_CON) is not the same as the MUS_ACT_CON. MUS_ACT_CON is counted in an improper way.	Contact your technical support.	Minor	NO	YES
AUD0129	VTRK_COUNT is not correct for IP set.Parameters: <TN>, <ACTIVECR>, <VTRK_COUNT>VTRK_COUNT is not calculated correctly due to a failure. It is modified to the correct value.	If the problem persists, contact your technical support.	Minor	NO	NO
AUD0130	The 'RX only' flag is TRUE, but ACTIVECR is NIL. The flag is set to FALSE.Parameters: <TN>The RX only flag is TRUE when the unit is idle, which is not allowed. It is reset to the proper value.	If the problem persists, contact your technical support.	Minor	NO	NO

BUG: Software Error Monitor

Message	Description	Action	Severity	Monitor	SNMP
BUG0752	SeaWeed memory library: Semaphore is owned by task <Task Name>, TID: <Task ID>, PC=<Program Counter>, PRIORITY=<Task Priority>, STATUS=<Task Status>Watchdog timer expires for some tasks, such as SL1.	Contact Nortel technical support.	Major	NO	YES
BUG0759	BSFE_TN_PTR is not NIL. Releasing memory allocated for BSFE_TN_BLOCK.	Contact your technical support group.	Minor	NO	YES
BUG0763	CHANNEL_TN is zero in procedure LINK_MSGCR.	Capture the bug message along with VNS D-channel traces and provide it to technical support to investigate further.	Minor	NO	NO
BUG0764	X: RFC call failed. Pointer to memory block: Y, Number of words: Z where X = the calling function name, Y = the memory pointer and Z = the number of words.	Contact your technical support.	Critical	YES	YES
BUG0765	sl1SegPdsAlloc: RFC get pdata request returns a NULL pointer.	Contact your technical support.	Critical	YES	YES

Message	Description	Action	Severity	Monitor	SNMP
BUG0766	sl1SegPdsAlloc: ptr address validation failed for ptr [X] where X is the pointer address	Contact your technical support.	Critical	YES	YES
BUG0767	Memory leak! sl1SegPdsFree function failed to free a protected memory block. Pointer to memory block to free: X, Number of words to free: Y where X is the pointer to free and Y is the number of words to free.	Contact your technical support.	Critical	YES	YES
BUG0768	sl1SegPdsFree: Pointer to memory block to free is null.	Contact your technical support.	Critical	YES	YES
BUG0769	Incorrect condition of the Inventory Sets task flags. INVSETSUSAGEFLAG will be reset. Parameters: INVABORTSETSFLAG, INV_SETS_PM, INV_SETSQID, INV_LOOP_INIT, INV_SHELF_INIT, INV_CARD_INIT, INV_UNIT_INIT		Info	NO	NO
BUG0778	Incorrect condition of the Inventory Cards task flags. INVCARDUSAGEFLAG will be reset. Parameters: INVABORTCARDFLAG, INV_CARD_PM, INV_CARDQID, INV_LOOP_INIT, INV_SHELF_INIT, INV_CARD_INIT, INV_UNIT_INIT		Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
BUG0779	The number of IP Attendant Consoles ISM counter corruption encountered. Counter is reset to zero.	Reconfigure the IP Attendant console.	Minor	NO	NO
BUG0792	TSKINHIB bit for OVLMANUAL task is set incorrectly for OVL 2.		Minor	NO	YES
BUG0867	CDM_SAVE_TN: Cannot obtain numbering zone.		Minor	NO	YES

CCBR: Customer Configuration Backup and Restore

Message	Description	Action	Severity	Monitor	SNMP
CCBR0032	New keycode is not activated because the newly configured ISM limit is less than the actual usage. Insufficient ISM limit configured on the new Keycode file.	Check the ISM Limit of the new keycode and adjust the value accordingly or Remove the extra data of the affected ISM from the system data.	Info	NO	NO
CCBR0033	The CCBR file is missing. Please generate the CCBR file by means of EDD CCBR in Overlay 43.	Use EDD CCBR in Overlay 43 to generate the CCBR file.	Info	NO	NO
CCBR0034	UDT upgrade Fail message arrived from MGC.UDT upgrade failed. <Loop n [l s c]> err <x>The MGC sends a message to the Call Server stating that the upgrade process of a certain	Wait a few minutes and then make another attempt to upgrade the UDT by issuing the UPGUDT command. If still not successful then unplug the UDT, plug it back in	Minor	NO	YES

Message	Description	Action	Severity	Monitor	SNMP
	UDT has failed. The UDT will reset and come up with its default factory loadw	its place, and after it resets make another attempt to upgrade it. If the problem persists, con			
CCBR0035	UDT upgrade Reject message arrived from MGC.UDT upgrade rejected. <Loop n [l s c]> err <x>The MGC sends a message to the Call Server stating that the MGC rejects the request to upgrade a certain UDT. The MGC will not send a command to the UDT to start	Contact your technical support group. If upgrading the UDT is not urgent then the UDT can be enabled and put back to service.	Minor	NO	YES
CCBR0036	UDT upgrade response timeout from MGC <detailed timeout condition>The CS encountered a timeout during the process of upgrading the UDT or during the process of aborting an existing UDT upgrade. If the UDT has received the complete loadware file then it	Wait for the UDT to completely reset. Enable the loop and query for the current version (by using the VER command in LD 60). If the old loadware version is still deployed, attempt to commit another upgrade by using the UPGUDT command in LD 143.	Minor	NO	YES
CCBR0037	No UDT upgrade currently exists; received UDT_ABORT_UPGRADE in UDT_UPG_ST_IDLE A request to abort a UDT upgrade was made, but the Call Server was not being upgraded.		Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
CCBR0038	UDT card must be disabled cab <cabNum>[l s c] Loop <digitsl loop number>A request to upgrade a UDT was made while the UDT was enabled. The upgrade request is ignored.	Disable the loop and try again to upgrade the UDT.	Info	NO	NO
CCBR0039	Internal failure in UDT upgrade process <failure details>The CS encountered an internal problem while handling a request to upgrade a UDT or abort an existing UDT upgrade process. If this problem happened before the UDT upgrade had started, the UDT may	If the reason for the error is a failure to find the loadware file, ensure that the loadware file exists. If the UDT loadware is patched, check that the loadware patch points to an existing file. For other failure reasons, wait for the UDT to complete it	Minor	NO	YES
CCBR0040	You cannot request a UDT upgrade for a non-UDT loop. A request for a UDT upgrade was made for a non-UDT loop. The request is ignored	Check the TN (loop, shelf, and card) of the UDT that you attempted to upgrade.	Info	NO	NO
CCBR0041	UDT upgrade message arrived in wrong state <detailed description>The UDT upgrade process received a message that is not expected to be received in the state in which it arrived. This is an informational message only. In	No action is needed. In case of an upgrade failure, this message will be followed by the appropriate specific failure message.	Minor	NO	YES

Message	Description	Action	Severity	Monitor	SNMP
	case of an upgrade failure, this				
CCBR0042	MSDL must be disabled <Loop x Shelf y Card z> A request for a UDT upgrade was made for a UDT loop which has an associated MSDL card in an enabled state. The upgrade request is ignored.	Disable both the MSDL and the UDT loop and try the UDT upgrade again.	Info	NO	NO

DTI: Digital Trunk Interface Diagnostic (LD 60)

Message	Description	Action	Severity	Monitor	SNMP
DTI0077	You cannot request a UDT version query for a non-UDT loop. A request for a UDT version query was made for a non-UDT loop. The request is ignored.	Check the TN (digital loop number) of the UDT to which the request is intended.	Info	NO	NO
DTI0078	Failed to send VID query to UDT. The CS failed to send a version query message to the appropriate loop. The request is ignored.	Ensure the digital loop number corresponds to a UDT pack.	Minor	NO	YES
DTI0079	Enable Loop request is not valid for a UDT loop while it is upgrading. A request was made to enable a loop that is a UDT that is currently being upgraded. The request is ignored.	Wait until the upgrade is completed, or request to abort the upgrade prior to enabling the loop.	Info	NO	NO

ERR: Error Monitor (Hardware)

Message	Description	Action	Severity	Monitor	SNMP
ERR0145	The Group Alert Feature only updates the displays for m sets. Including MADNs hunting list n has x members.		Info	NO	NO
ERR0146	Failed to find the Zone-Based Country Code CLID may be incorrect on set display for international calls.	Check that correct ZBD zone is used for the set. Check the ZBD zone in LD 117 If the problem persists, please contact your technical support.	Major	YES	YES
ERR0147	Looping of calls due to active Single Number Mobile Number feature(SNMN); call aborted. Calls in the loop will not land on any set and the originating side will get an overflow tone.	Check your configuration to avoid the loop call scenario.	Major	YES	YES
ERR0148	CLID generation failed. <TN> <PTN> <CAUSE>	Contact your technical support. To assist in diagnosing the problem, gather the following information: • Call Server logs • MGC logs	Major	YES	YES
ERR0149	Received disconnect with cause code 3 or 28 or 34 in ALERTING state. MALT cannot be triggered and	No action required.	Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
	MALT_INFO flag is cleared.				
ERR0151	MALT triggered due to network failure in ALERTING state. Potential call failures may result, if the destination is not reachable through any other routes, or if the destination user answers the call during the interval between failure and the new attempt.		Info	NO	NO
ERR0152	Route List Block entry with Local Termination Continuation can not be used for CDP call. NARS Local Termination Continuation is blocked for CDP call	Check that RLI with LTER CONA=YES is not used for CDP configuration.	Major	YES	YES
ERR0153	NARS Local Termination Continuation process failed. Current call is blocked for Continue Local Termination.	If the problem persists, contact your technical support group.	Major	YES	YES
ERR0154	Missing LTER Son call register. Current call is blocked for Continue Local Termination	If the problem persists, contact your technical support group.	Major	YES	YES
ERR0155	The IP Attendant codec list is empty. Attendant calls to this Attendant will fail.	Close the Attendant client application and reconnect. If the problem persists, check the MAS used to provide Attendant connections.	Major	NO	YES

Message	Description	Action	Severity	Monitor	SNMP
ERR5706	HOT P key configured as E.164 INTL DN, MSCO_DP is set to PUB/MIX but DIDN is NO. Parameters: <UEXT TN>E164 feature does not work for this TN.	Configure the HOT P key or MSCO_DP prompt properly.	Major	YES	YES
ERR5707	HOT P key configured as E.164 INTL DN but MSCO_DP is PRV.Parameters: <UEXT TN>E164 feature does not work for this TN.	Configure the HOT P key or MSCO_DP prompt properly.	Major	YES	YES

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

Message	Description	Action	Severity	Monitor	SNMP
ESN0057	Only digits or the characters 'p', 'c' and 'x' are allowed.		Info	NO	NO
ESN0059	OFFC code can only be from 1 to 7 digits in length.	Enter the correct number of digits.	Info	NO	NO
ESN0087	All OFFC code entries must contain the same number of digits.	Enter the correct number of digits.	Info	NO	NO
ESN0088	Route List Entry with LTER CONA is not supported for TSC and DSC configuration. TSC or DSC must not use a route list block that has LTER CONA = YES	Ensure the CONA is not set to YES in Overlay 86.	Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
ESN0089	The Digit Manipulation Index (DMI) with AC1/AC2 inserted is not allowed for LTER CONA = YES.	Ensure AC1/AC2 is not inserted with the DMI.	Info	NO	NO
ESN0121	The CNV is reset to NO. CNV must be NO for LTER CONA = YES	No user action is required; the CNV value is automatically reset.	Info	NO	NO
ESN0245	CMDB table number out of Range (1-256).	Enter a number in the range 1 to 256.	Info	NO	NO
ESN0246	CMDB table does not exist.	Enter a number for a table that does exist.	Info	NO	NO
ESN0247	CMDB table already exists.	Enter a new table number.	Info	NO	NO
ESN0248	CMDB rule does not exist	Enter a rule number that does exist.	Info	NO	NO
ESN0249	You cannot delete the Final Rule in a CMDB table.	Delete the table instead.	Info	NO	NO
ESN0250	You are not allowed to reduce the MXCM value below the configured table value.	Delete the table number greater than the MXCM value you are changing.	Info	NO	NO
ESN0251	MXCM value is out of range.	Enter a value in the range 1 to 255.	Info	NO	NO
ESN0252	Wrong number of arguments for the RLNO prompt.	Enter the correct number of arguments for the RLNO prompt.	Info	NO	NO

ITG: Integrated IP Telephony Gateway

Message	Description	Action	Severity	Monitor	SNMP
ITG5107	Proxy Server / Redirect Server <ServerIP:port> unreachable.Not able to reach specified server.	Contact your technical support group.	Cleared	NO	YES

LNK: Link Diagnostic (LD 48)

Message	Description	Action	Severity	Monitor	SNMP
LNK0242	The command can not be executed because no ELAN is configured.	Configure at least one ELAN.	Info	NO	NO

MGC: Media Gateway Controller

Message	Description	Action	Severity	Monitor	SNMP
MGC0019	MG1010 <supl> <sh> Power Supply unit error occurred.A fault has occurred on one of the 2 power supply units of the MG1010 cabinet indicated by <supl> <sh>.	Check the power supply to the power supply unit where the error has occurred. If you are not able to correct, contact technical support.	Major	YES	YES
MGC0020	MG1010 <supl> <sh> Power Supply unit error cleared.A fault that had	Monitor the power supply for additional errors	Cleared	NO	YES

Message	Description	Action	Severity	Monitor	SNMP
	occurred on one of the 2 power supply units of the MG1010 cabinet indicated by <supl> <sh> has been cleared.	and replace if the problem persists.			
MGC0021	MG1010 <supl> <sh> Ring Generator/Message Waiting voltage error occurred.A fault has occurred on the ring generator/message waiting voltage in the MG1010 cabinet indicated by <supl> <sh>.	Check the MGU card on the MG1010 cabinet.	Major	YES	YES
MGC0022	MG1010 <supl> <sh> Ring Generator/Message Waiting voltage error has cleared.A fault that had occurred on the ring generator/ message waiting voltage in the MG1010 cabinet indicated by <supl> <sh> has been cleared.	Monitor the Ring Generator for additional errors and replace if the problem persists.	Cleared	NO	YES
MGC0023	MG1010 <supl> <sh> Fan <fan number> failed.A fault has occurred on one of the 3 fans on MG1010. The fan number is indicated by <fan number> and cabinet indicated by <supl> <sh>.	Check the fan for reported failure.	Major	YES	YES
MGC0024	MG1010 <supl> <sh> Fan <fan number> recovered.One of the 3 fans that had failed has recovered	Monitor the Fan Unit for additional errors and replace if the problem persists.	Cleared	NO	YES

Message	Description	Action	Severity	Monitor	SNMP
	on the MG1010. The fan number is indicated by <fan number> and cabinet indicated by <supl> <sh>.				
MGC0025	MG1010 <supl> <sh> ambient temperature reached alarm temperature.Abmbient temperature of MG1010 cabinet indicated by <supl> <sh> has reached alarm temperature at 52C.	Check the reason for increase in temperature and rectify.	Major	YES	YES
MGC0026	MG1010 <supl> <sh> ambient temperature below alarm temperature.Ambient temperature of MG1010 cabinet indicated by <supl> <sh> has lowered from alarm temperature of 52C.	Check the reason for increase in temperature and rectify.	Cleared	NO	YES
MGC0027	MG1010 <supl> <sh> fans running at maximum speed.Operating conditions are approaching the cooling capacity of the chassis. Fans on the MG1010 have reached maximum speed. MG1010 cabinet indicated by <supl> <sh>.	Check reason for increase in temperature and rectify.	Warning	YES	YES
MGC0028	MG1010 <supl> <sh> fans speed lowered from maximum speed.Fans on the MG1010 reduced	Check the reason for increase in temperature and rectify.	Cleared	NO	YES

Message	Description	Action	Severity	Monitor	SNMP
	speed from maximum speed. MG1010 cabinet indicated by <supl> <sh>.				
MGC0029	MG1010 <supl> <sh> MGU card unplugged.The MGU card has been unplugged from the MG1010 cabinet indicated by <supl> <sh>.	Plug the MGU card back into the MG1010 cabinet.	Major	YES	YES
MGC0030	MG1010 <supl> <sh> MGU card plugged in.The MGU card has been plugged in to the MG1010 cabinet indicated by <supl> <sh>.	No action required.	Cleared	NO	YES

MSC: Media Services

Message	Description	Action	Severity	Monitor	SNMP
MSC2000	MSC did not receive a response from the server <ServerIP:port>.The media service will not be provided due to timeout response trying to reach the specified server.	Contact your technical support group.	Major	NO	YES

NPR: Network and Peripheral Equipment Diagnostic (LD 32)

Message	Description	Action	Severity	Monitor	SNMP
NPR0059	This command is not applicable for DTR Card. This will affect the associated DB128 VGW units on CARD 9, 10 and 15, if configured.	Use LD34 commands for DTR.	Info	NO	NO

OSM: Operating System Messaging

Message	Description	Action	Severity	Monitor	SNMP
OSM0034	New coredump on the system. When an application crashes a new coredump file is created on the system. This file includes information which is useful for applications issue investigation.	Check the /var/coredump/ directory and save the core dump file. Retrieve the application name from the coredump file name and ensure that the application is enabled on the system.	Major	YES	YES
OSM0035	Monit found <APPNAME> application stopped.Monit will try to start <APPNAME> application.	Check the corresponding application log file.	Major	YES	YES
OSM0036	Monit found <APPNAME> application unresponsive.Monit will try to restart	Check the corresponding application log file.	Major	YES	YES

Message	Description	Action	Severity	Monitor	SNMP
	<APPNAME> application.				

SCH: Service Change

Message	Description	Action	Severity	Monitor	SNMP
SCH2360	Non-zero group number entered but feature is disabled in CDB (OPT = GPAD).	Set GPA option in CDB FTR_DATA to GPAA	Info	NO	NO
SCH2364	Enter the multi configuration value in the following range: DTR/XTD: 2 to 8 MFR: 2 to 4 CMOD: 2 to 32	Enter the multi configuration value within the allowed range for the respective card.	Info	NO	NO
SCH2366	The deflect key is already defined. Only one DFLC key is allowed for each set.		Info	NO	NO
SCH2367	The deflect key can be configured for ethersets only.		Info	NO	NO
SCH2368	DB32 cannot be configured on card slot 0 for this IPMG type. The TYPE DB32 is not supported on card slot 0 for MGS type IPMG, as only card slots 11, 12 and 13 are used.	Configure DB32 on card slot 11.	Minor	NO	NO
SCH2369	The MUTA/MUTD class of services can be configured for ethersets with mute key only.		Info	NO	YES

Message	Description	Action	Severity	Monitor	SNMP
SCH2370	Input is applicable for ethersets only.		Minor	NO	NO
SCH2371	Further operations (Add/Delete) aborted because the maximum limit of units for the card was reached.		Info	NO	NO
SCH2372	The number of IP Attendant Consoles TNs in the system exceeds the maximum number allowed.	Review ISM and purchase new if required.	Info	NO	NO
SCH2373	DVLA CLS can not be set for TN block with the configured directory number.	Configure a new IP set without a DN or remove the DN.	Info	NO	NO
SCH2374	DN can not be configured for DVLA sets.	Configure a new IP set or set DVLD CLS.	Info	NO	NO
SCH2375	3260 IP Attendant sets have to be defined on virtual super loops.	Configure 3260 IP Attendant with a Virtual TN.	Info	NO	NO
SCH2376	More than 1000 records received in STIP DVLA report. Only 1000 records will be printed. Only 1000 records can be printed at once.	Specify a larger idle time parameter for the STIP DVLA command.	Info	NO	NO
SCH2377	DB128 configuration is allowed only on CARD 0, 9, 10, 11, 12,13, 14 and 15.	Add DB128 to CARD 0, 9, 10, 11, 12,13, 14 and 15.	Info	NO	NO
SCH2378	DB128 configuration is not allowed on this card. Configuration of DB128 is allowed only on slot 0, 9, 10. 11, 12, 13, 14, and 15.	Add DB128 to CARD 0, 9, 10, 11, 12,13, 14 and 15.	Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
SCH2379	DB128 configuration is not allowed on MGX IPMG. MGX supports only DB96 configuration.		Info	NO	NO
SCH2380	You have reached the maximum number of TNs allowed for this category.		Info	NO	NO
SCH2381	ICRA/ICRD class of service no longer exists; these CLS are replaced with RECA/RECD respectively.	Configure RECA/ RECD instead of ICRA/ICRD.	Info	NO	NO
SCH2382	Trunks must be removed before changing the Route.	Remove all the trunks associated with the Route and change the field.	Info	NO	NO
SCH2383	The route data block cannot be deleted while there are sets associated with it (check MRT of sets).	Remove all references to RDB in sets configuration from MRT.	Info	NO	NO
SCH2384	There are too many sets associated with this route. No more sets can have this route assigned.	Create another route and assign it to a set.	Info	NO	NO
SCH2385	Configuration not allowed on this card. Maximum virtual DTR/XTD/MFC/MFE per IPMG is two.		Info	NO	NO
SCH2386	There are system park DNs.		Info	NO	NO
SCH2387	System park DN cannot be deleted if Call Park option is CPA.	Change Call Park option to CPD in LD 15 and try again or new range must completely cover system park DNs.	Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
SCH2388	Active park DNs cannot be deleted.	Try again later or new range must completely cover system park DNs.	Info	NO	NO
SCH2389	Warning: Group Call List includes originator DN. Group Call originated by the set to this group may work incorrectly. <Group Call Key> <DN>	Remove the group call key, remove the DN key, or change the group call list.	Info	NO	NO
SCH2390	Warning: duplicated DN is found and removed from the group call list. <DN>		Info	NO	NO
SCH2391	Warning: some DNs in the group call list were shifted to the left. DNs were shifted in order to occupy only the left-most entries of the group call list.		Info	NO	NO
SCH2392	Out of range (0-8000). Configuration of MBXT is not allowed with value out of range.	Use a timer value within the range 0-8000.	Info	NO	NO
SCH2393	Unable to perform Dialing Configuration for default Zone 0.		Info	NO	NO
SCH2394	DB96 cannot be configured for this IPMG type. DB96 is not supported on MGS Type IPMG; only DB32 and DB128 are supported.	Configure either DB32 or DB128 on MGS IPMG type	Minor	NO	NO
SCH2395	DB128 can be configured only on cards 11, 12, 13 and	Configure DB128 on card slots 11, 12, 13, 14.	Minor	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
	14 for MGS type IPMG.				
SCH2396	Only UEXT sets can be configured with the ELMA/ELMD class of service.	Configure ELMA/ ELMS on UEXT set type.	Info	NO	NO
SCH2397	This UEXT cannot be configured with the ELMA class of service.		Info	NO	NO
SCH2398	There is already a UEXT with the ELMA class of service in the MADN group. Only one UEXT can be configured with the ELMA class of service in the MADN group.	Change ELMA to ELMD for the other UEXT in the MADN group or for this UEXT.	Info	NO	NO
SCH2399	IP Media Services Package is not equipped.	Enable package 422.	Info	NO	NO
SCH2400	Invalid entry for TON prompt (MSRN).	Select one of the following valid TON values: INTL, NATL, ESPN, LOCL, ELOC, ECDP.	Info	NO	NO
SCH2401	Invalid entry for MSRN prompt. MSRN input can be up to 24 digits long.	Add valid MSRN.	Info	NO	NO
SCH2402	Invalid entry for NPI prompt (MSRN).	Enter one of the following valid NPI values: E164, PRIV.	Info	NO	NO
SCH2403	Line <line number> cannot be parsed. Last parsed zone – <zone number>The zone.csv file contains incorrect data.		Warning	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
SCH2404	Insufficient number of IP RAN ISM connections. The IP Ran sessions ISM limit has been reached.	Increase the number of IP RAN ISMs. An inrease in the following ISMs and license may also be required: 1. IP Media Services Session license on the CS 1000. 2. CS 1000 RFC 4240 Services Sessions on the Media Application Server (MAS).	Warning	NO	NO
SCH2405	Insufficient number of IP MUS ISM connections. The IP Mus sessions ISM limit has been reached.	Increase the number of IP MUSIC ISMs. An increase in the following ISMs and license may also be required: 1. IP Media Services Session license on the CS 1000. 2. CS 1000 RFC 4240 Services Sessions on Media Application Server (MAS).	Warning	NO	NO
SCH2406	Insufficient number of ISM connections to change a MUS route to broadcasting. The ISM MUS connections limit has been reached.		Warning	NO	NO
SCH2407	The number of IP Media Services in the system exceeds the maximum number allowed. The IP Media Services sessions ISM limit has been reached.	Increase the number of IP Media Services Session licenses on the CS 1000	Warning	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
SCH2408	Insufficient number of MUS ISM connections. The Mus sessions ISM limit has been reached.	Increase the number of IP MUSIC ISMs. An increase in the following ISMs and license may also be required: 1. IP Media Services Session license on the CS 1000. 2. CS 1000 RFC 4240 Services Sessions on Media Application Server (MAS).	Warning	NO	NO
SCH2409	Trunk limit exhausted. The maximum number of H323 trunks that can be configured is 1200.		Minor	NO	NO

SEC: Security Notification Monitor

Message	Description	Action	Severity	Monitor	SNMP
SEC0122	Ports used for the NFS service are blocked by the firewall.	Check that the changes were done by an authorized person.	Cleared	NO	YES
SEC0123	Ports used for the NFS service are not blocked by the firewall. This is a potential security exposure.	Check that the changes were done by an authorized person.	Major	YES	YES

SRPT: System Reports

Message	Description	Action	Severity	Monitor	SNMP
SRPT0328	There is more than one element configured as Leader in the node. There should only be one Leader in the node	Configure only one Leader in the node	Info	NO	NO
SRPT0329	The file /e/inactive.dr is found. Marking the disk status as BAD. The last disk sync was not complete.	This condition will be cleared when the remote core comes up as active and performs another disk sync. Bring up the remote core as redundant active. You may need to perform a cutover followed by join if the current side has come up as active.	Minor	NO	NO
SRPT0330	Sending to cpmLocMsgQid <id> failed, errno: <errno>.Sending messages to the Message Queue cpmLocMgQid failed.	If the error message disappears after 3 or 4 occurences, then no action is required. If it appears continously, then contact your technical support.	Minor	NO	NO
SRPT0331	<tool name> / tool number <tool number> in toolbox has been activated by the user.Tool name is the name (a string) of the tool activated. Tool number is an integer		Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
	value corresponding to the tool.Indicates a tool is activated by the user.				
SRPT0332	<tool name> / tool number <tool number> in toolbox has been deactivated by the user.Tool name is the name (a string) of the tool activated. Tool number is an integer value corresponding to the tool.Indicates a tool is de-activated by the user.		Info	NO	NO
SRPT0333	<tool name> / tool number <tool number> in toolbox has been deactivated by the the system due to timer expiration.Tool name is the name (a string) of the tool activated. Tool number is an integer value corresponding to the tool.Indicates a tool is de-		Info	NO	NO
SRPT0334	<tool name> / tool number <tool number> in toolbox has been permitted by the user.Tool name is the name (a string) of the tool activated. Tool number is an integer value corresponding to the tool.Indicates a tool is permitted by the user.		Info	NO	NO
SRPT0335	<tool name> / tool number <tool number>, in toolbox		Info	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
	is no longer permitted by the user.Tool name is the name (a string) of the tool activated. Tool number is an integer value corresponding to the tool.Indicates a tool is no longer permitted.				
SRPT0336	HSEM invalid db format. The /u/db/hsem.db file is corrupted.	Check the Element Manager transaction history to ensure transaction integrity. The next EDD should update the file. If the problem persists, contact your technical support group.	Major	YES	YES

SYS: System Loader

Message	Description	Action	Severity	Monitor	SNMP
SYS0175	The number of IP Attendant Console TNs exceeds the IP Attendant Consoles limit and no further TNs can be sysloaded.	Contact your technical support group.	Critical	YES	YES
SYS0176	UID data block tn = 0. TN is 0 when loading UID data during SYSLOAD.	Contact Field Support	Major	NO	NO
SYS0177	UID data block pointer is NIL. The UID data block pointer is NIL when	Contact Field Support	Major	NO	NO

Message	Description	Action	Severity	Monitor	SNMP
	loading the data during SYSLOAD.				
SYS0179	Data associated with an obsolete feature or unsupported hardware has been detected and removed from the system. Dependent data may also be deleted and reported with other error messages.	Verify that the remaining data is correct and then perform EDD CLR in overlay 43.	Minor	NO	YES
SYS0180	IP Media Services package is not equipped. Data has been removed.	Add the IP Media Services package 422 if the IP data is needed.	Info	NO	NO

TEMU: Tape Emulation

Message	Description	Action	Severity	Monitor	SNMP
TEMU0034	The Element Manager transaction record file <file path and name> is missing. Errno = [0x %x]The file is missing. It may be due to software installation/upgrade. It is created after the first database backup.	This message can be ignored if it appears right after software installation/ upgrade. This file will be created after the first database backup operation. If this message persists, please contact your technical support.	Minor	NO	NO

TFC: Traffic Control (LD 2)

Message	Description	Action	Severity	Monitor	SNMP
TFC0217	Threshold value for CDR Record Loss is 0 and is not configurable.		Info	NO	NO