
Nortel Communication Server 1000

Nortel Communication Server 1000 Release 7.0

Communication Server 1000E

Software Upgrades

Document Number: NN43041-458

Document Release: 04.03

Date: July 2010

Copyright © 2004-2010 Nortel Networks. All rights reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Contents

List of procedures	9
New in this release	13
Features	13
Other	13
Revision History	13
How to get help	17
Getting help from the Nortel Web site	17
Getting help over the telephone from a Nortel Solutions Center	17
Getting help from a specialist by using an Express Routing Code	18
Getting help through a Nortel distributor or reseller	18
Finding the latest updates on the Nortel web site	19
System Information	21
Subject	21
Applicable systems	21
Intended audience	21
Conventions	22
Related information	23
Technical support	24

Overview	25
Contents	25
Communication Server 1000 task flow	26
Co-resident Call Server and Signaling Server	28
References in preparation for an upgrade	28
CS 1000 Release 7.0 software upgrades	28
System types	29
Backwards/forwards compatibility	29
MG 1000T upgrade and migration options	30
Option 1	30
Option 2 (recommended)	31
Conversion and mapping information	31
Cabinet or Chassis to IPMG mapping	31
TN mapping	32
XNET and XPEC conversion	39
TTY conversion	39
Tone Receiver Conversion	40
Conference and Tone Generator conversion	41
IPMG Configuration	42
DSP Resources for IPMGs	42
Deleted information	43
Campus Redundancy (High Availability) Package Support	43
Additional factors for consideration	43
SSC Security Device (dongle) considerations	43
NARS/BARS/Trunking Considerations	44
Media Gateway considerations	45
NRS considerations	45
Signaling Server considerations	45
ELAN, TLAN and IP considerations	46
Estimating installation time	46
Administration tools	47
Element Manager	48
Network Time Protocol (NTP)	49
Simple Network Management Protocol (SNMP)	49

Upgrading the Signaling Server	50
Recorded Announcement and Music	50
H.323 Gatekeeper database migration	50
Passwords	50
First steps	53
Contents	53
Things to know	53
CS 1000 Release 7.0 product compatibility	53
Software requirements	60
Keycodes	61
What to have ready	62
Data checklist	62
Readiness checklist	63
First steps	65
Co-resident Call Server and Signaling Server	67
Contents	67
Overview	67
Supported configurations	68
Co-res CS and SS based CS 1000E system	68
Co-res CS and SS based Branch Office Media Gateway	69
Communication Server 1000E TDM	70
High Availability (HA) support	71
Co-res CS and SS upgrade paths	71
Hardware	71
CP PM upgrade kit	72
CP PM media storage	72
CP MG, CP DC, and COTS2 media storage	73
Software applications	73
Element Manager	74

Upgrading Call Server software (CP PIV, CP PM)	75
Contents	75
Introduction	75
Software pre-conversion	76
Preparing for the upgrade	76
Planning	77
Upgrade Checklists	78
Preparing	78
Pre-upgrade checklists	79
Pre-upgrade checklists for Geographic Redundant Survivable sites ..	83
Making a bootable RMD	87
Connecting a terminal	96
Printing site data	97
Performing a template audit	100
Backing up the database (CP PIV and CP PM data dump)	101
Performing the upgrade	103
Reviewing upgrade requirements	103
Software Install Kits	103
Splitting the Call Servers	104
Upgrading to CS 1000E Release 7.0 (CP PIV or CP PM)	106
Verifying the upgraded database	123
Reconfiguring I/O parameters and call registers	127
Switching call processing to Call Server 1	128
Upgrade the Voice Gateway Media Card loadware	129
Upgrading the software on Call Server 0	129
Making the system redundant	130
Register the Call Server to the security domain	130
Logoff and login to the Call Server	130
Completing the upgrade	131
Testing the Call Servers	131
Switching call processing	134
Upgrading the Signaling Server	137
Contents	137

Taskflow	138
Supported hardware	140
IP subnet configuration	140
ISP1100 migration	140
Upgrading and reconfiguring the software	140
NRS	140
Determining the IP Phone firmware version	141
Performing the software upgrade	141
Upgrading and distributing IP Phone firmware	141
Upgrading Voice Gateway Media Cards	143
Contents	143
Things to know	143
Gateway Controller loadware	144
Task summary	146
Verify current loadware versions	146
Determine Voice Gateway Media Card loadware version	147
Obtain and upload loadware files	151
Upgrade the Voice Gateway Media Card loadware	154
Upgrade loadware using a Software Delivery card	158
Installing a new keycode	161
Contents	161
Introduction	161
Feature operation	162
Co-resident Call Server and Signaling Server keycode validation and pre-configuration	163
Feature and License parameter upgrade using a keycode delivered on a CF card	164
Feature and License parameter upgrade using HyperTerminal®	169
Feature and License parameter upgrade entered manually	171
Reverting to the previous keycode with the KRVR command	173

Upgrade checklists	177
Contents	177
Introduction	177
Technical Support	177
Site details	178
Upgrade details	178
Pre-upgrade checklists	179
Software Upgrade	179
Hardware Upgrade	185
Pre-conversion steps	185
Post-conversion checks	187
Appendix A: Obtaining software	189
Downloading software from the Nortel website	189
Technical Assistance service	191
Contents	191
Nortel Technical Assistance Centers	191
Services available	194
Requesting assistance	197

List of procedures

Procedure 1	
Preparing for upgrade	65
Procedure 2	
Pre-upgrade activities	79
Procedure 3	
Pre-upgrade activities for GR Survivable sites	85
Procedure 4	
Upgrading a GR Survivable system	85
Procedure 5	
Creating a bootable Call Server software CF card	88
Procedure 6	
Connecting a terminal	96
Procedure 7	
Performing a data dump to backup the customer database:	101
Procedure 8	
Checking that Call Server 0 is active	105
Procedure 9	
Splitting the Call Servers	106
Procedure 10	
Upgrading the software (CP PIV or CP PM)	106
Procedure 11	
Verifying the upgraded database	123
Procedure 12	
Reconfiguring I/O ports and call registers	127
Procedure 13	
Switching call processing	129
Procedure 14	
Making the system redundant	130

Procedure 15	
Registering the Call Server to the security domain	130
Procedure 16	
Testing Call Server 0	131
Procedure 17	
Switching call processing	132
Procedure 18	
Testing the Call Server	133
Procedure 19	
Switching call processing	134
Procedure 20	
Performing a data dump to backup the customer database:	134
Procedure 21	
Determining loadware version during boot sequence	147
Procedure 22	
Determining the loadware version through Element Manager	147
Procedure 23	
Determining the loadware version through the CLI	150
Procedure 24	
Obtaining and uploading loadware and firmware	152
Procedure 25	
Upgrading Voice Gateway Media Card loadware	154
Procedure 26	
Upgrading loadware using a Software Delivery card	159
Procedure 27	
Performing a feature and License parameter upgrade using a keycode delivered on a CF card.	164
Procedure 28	
Performing a feature and License parameter upgrade	169
Procedure 29	
Performing a feature and License parameter upgrade manually	171
Procedure 30	
Revert to old keycode	173
Procedure 31	
Parallel reload for CP PIV and CP PM	174

Procedure 32
Downloading software from the Nortel website 189

New in this release

Features

Communication Server 1000E Standard Availability and High Availability local VxWorks based software upgrade procedures remain the same as the previous release.

There have been no updates to the feature descriptions in this document.

Other

Revision History

July 2010

Standard 04.03. This document is up-issued to revise the command to join a Call Server to the UCM Security Domain.

June 2010

Standard 04.02. This document is up-issued to include a CS 1000E task flow and CP PM version 2 content.

June 2010

Standard 04.01. This document is issued to support Communication Server 1000 Release 7.0.

February 2010

Standard 03.12. This document is up-issued to support Communication Server 1000 Release 6.0

January 2010

Standard 03.11. This document is up-issued to support Communication Server 1000 Release 6.0

January 2010

Standard 03.10. This document is up-issued to support Communication Server 1000 Release 6.0

December 2009

Standard 03.09. This document is up-issued to support Communication Server 1000 Release 6.0

December 2009

Standard 03.08. This document is up-issued to support Communication Server 1000 Release 6.0.

December 2009

Standard 03.07. This document is up-issued to support Communication Server 1000 Release 6.0.

October 2009

Standard 03.06. This document is up-issued to support the Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card.

September 2009

Standard 03.05. This document is up-issued to support the Media Gateway 1010.

June 2009

Standard 03.04. This document is up-issued for Communication Server 1000 Release 6.0.

June 2009

Standard 03.03. This document is up-issued for Communication Server 1000 Release 6.0.

May 2009

Standard 03.02. This document is up-issued for Communication Server 1000 Release 6.0.

May 2009

Standard 03.01. This document is up-issued for Communication Server 1000 Release 6.0.

September 2008

Standard 02.04. This document is up-issued for Communication Server 1000 Release 5.5.

April 2008

Standard 02.03. This document is up-issued for Communication Server 1000 Release 5.5.

March 2008

Standard 02.02. This document is up-issued for Communication Server 1000 Release 5.5.

December 2007

Standard 02.01. This document is up-issued for Communication Server 1000 Release 5.5.

July 2007

Standard 01.06. This document is up-issued for Communication Server 1000 Release 5.0.

June 2007

Standard 01.05. This document is up-issued with corrections from CR Q001597896.

June 2007

Standard 01.04. This document is up-issued with corrections from CR Q001597896.

June 2007

Standard 01.03. This document is up-issued with corrections from CR Q001620560.

June 2007

Standard 01.02. This document is up-issued with corrections from CR Q001650872.

May 2007

Standard 01.01. This document is up-issued for Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: *Communication Server 1000E: Upgrade Procedures* (553-3041-258).

August 2005

Standard 2.00. This document is up-issued to support CP PIV and Communication Server 1000 Release 4.5.

September 2004

Standard 1.00. This document is issued for Communication Server 1000 Release 4.0.

How to get help

This section 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:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- 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 don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone 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 phone number for your region:

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:

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.

Finding the latest updates on the Nortel web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for CS 1000 Release 7.0, click one of the links below.

Latest Software	Takes you directly to the Nortel page for CS 1000 Release 7.0 software.
Latest Documentation	Takes you directly to the Nortel page for CS 1000 Release 7.0 documentation.

System Information

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

Subject

This document provides procedures for upgrading a Communication Server 1000E (CS 1000E) system to Nortel Communication Server Release 7.0 software.

Note on legacy products and releases

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

www.nortel.com

Applicable systems

This document applies to CS 1000E systems.

Intended audience

This guide is intended for system installers and administrators with a strong understanding of CS 1000E equipment and operation. Contact Nortel Training Centers for information on installation courses.

Conventions

In this document, CS 1000E systems are referred to generically as system.

The following systems are referred to generically as Small system:

- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 11C Chassis
- Communication Server 1000S (CS 1000S)

The following hardware is referred to generically as Media Gateway:

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

The following cards are referred to generically as Gateway Controller:

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

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

- Call Processor Pentium IV (CP PIV)
- Common Processor Pentium Mobile (CP PM)
- Common Processor Media Gateway (CP MG)
- Common Processor Dual Core (CP DC)
- Commercial off-the-shelf (COTS) servers

- IBM x306m server (COTS1)
- HP DL320 G4 server (COTS1)
- IBM x3350 server (COTS2)
- Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

The following table shows CS 1000 Release 7.0 supported roles for common hardware platforms.

Table 1
Hardware platform supported roles

Hardware platforms	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PIV	yes	no	no	no
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	no	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS1	no	yes	no	no
COTS2	no	yes	yes	no

Note: The CP MG card functions as the Co-resident Call Server and Signaling Server, and the Gateway Controller while occupying Slot 0 in a Media Gateway.

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Communication Server 1000E Hardware Upgrade Procedures* (NN43041-464)
- *Converging the Data Network with VoIP* (NN43001-260)
- *Signaling Server IP Line Application Fundamentals* (NN43001-125)
- *IP Peer Networking: Installation and Commissioning* (NN43001-313)
- *Branch Office: Installation and Commissioning* (NN43001-314)
- *Element Manager: System Administration* (NN43001-632)
- *IP Phones Fundamentals* (NN43001-368)
- *Communication Server 1000E: Overview* (NN43041-110)
- *Communication Server 1000E: Planning and Engineering* (NN43041-220)
- *Communication Server 1000E: Installation and Commissioning* (NN43041-310)
- *Network Routing Service Fundamentals* (NN43001-130)

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support** on the Nortel home page:

www.nortel.com/

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Technical support

For technical support contact information, see “Technical Assistance service” on [page 191](#).

Overview

Contents

This section contains information on the following topics:

Communication Server 1000 task flow	26
Co-resident Call Server and Signaling Server	28
References in preparation for an upgrade	28
Backwards/forwards compatibility	29
CS 1000 Release 7.0 software upgrades	28
Backwards/forwards compatibility	29
Conversion and mapping information	31
Campus Redundancy (High Availability) Package Support	43
Additional factors for consideration	43
Estimating installation time	46
Administration tools	47
Upgrading the Signaling Server	50
Recorded Announcement and Music	50
H.323 Gatekeeper database migration	50
Passwords	50

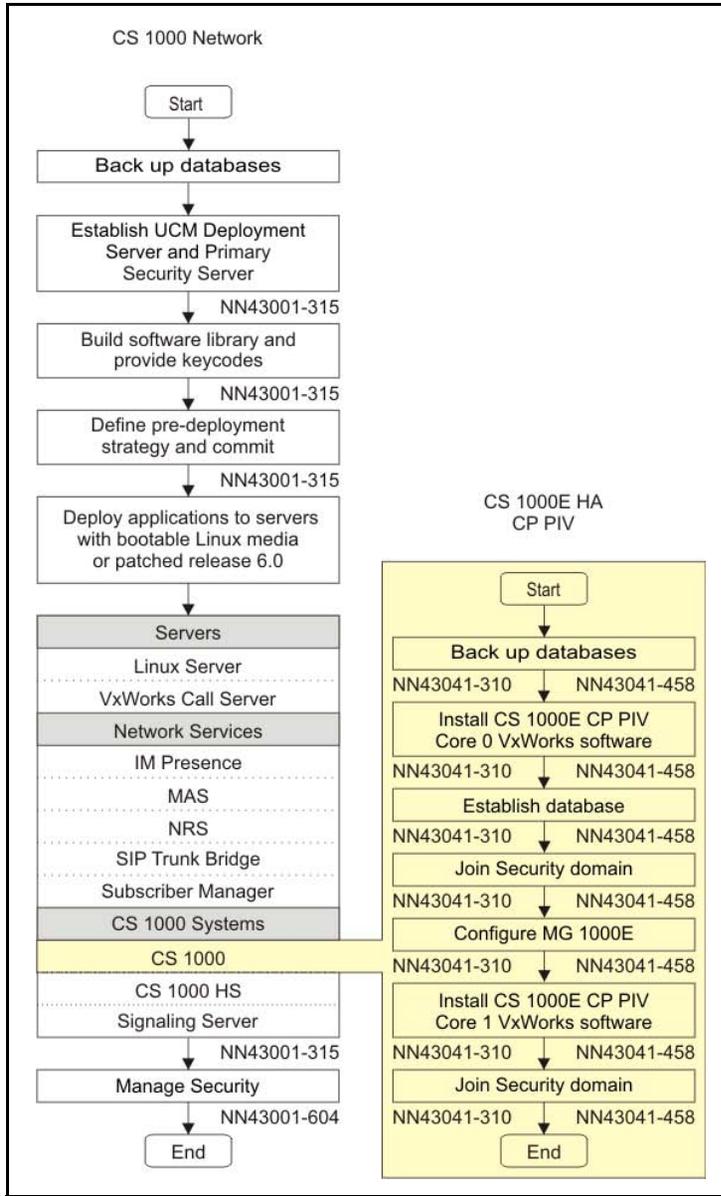
Communication Server 1000 task flow

This section provides a high-level task flow 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.

For more information refer to the following NTPs, which are referenced in Figure 1 on [page 27](#):

- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Security Management* (NN43001-604)

Figure 1
Communication Server 1000E task flow



Co-resident Call Server and Signaling Server

A CS 1000 system consists of two major functional components: a Call Server and a Signaling Server. These two components have historically run on separate Intel Pentium processor-based hardware platforms operating under the VxWorks Operating System.

The Co-resident Call Server and Signaling Server (Co-res CS and SS) can run the Call Server software, the Signaling Server software, and System Management software together on one hardware platform running the Linux Base Operating System. Various hardware platforms support the Co-res CS and SS configuration. For more information on supported hardware platforms, see Table 1: “Hardware platform supported roles” on [page 23](#).

References in preparation for an upgrade

To plan the network, see *Communication Server 1000E Planning and Engineering* (NN43041-220) and *Converging the Data Network with VoIP* (NN43001-260).

To read about installing, configuring, and managing Voice Gateway Media Cards and IP Phones, see *Signaling Server IP Line Application Fundamentals* (NN43001-125) and *IP Phones Fundamentals* (NN43001-368).

For detailed information about installing and configuring new components, see *Communication Server 1000E Installation and Commissioning* (NN43041-310) and *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

To read about virtual trunking and the Network Routing Service (NRS), see *Network Routing Service Fundamentals* (NN43001-130), *IP Peer Networking Installation and Commissioning* (NN43001-313) and *Communication Server 1000E Overview* (NN43041-110).

CS 1000 Release 7.0 software upgrades

This document provides information on Communication Server 1000E Release 7.0 local VxWorks software upgrades for CP PIV and CP PM based systems.

For information on local Linux Base software upgrades, or Deployment Manager upgrades, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)

For detailed information about Co-resident Call Server and Signaling Server supported upgrade paths, see “Co-resident Call Server and Signaling Server” on [page 67](#).

If you are upgrading from a system that is not supported in CS 1000 Release 7.0, see the appropriate legacy documentation.

System types

Table 2 lists the various system types according to processor type.

Table 2
System types (Release 7.0 software)

Processor Type	System Type		
	Option 61C CS 1000M	Option 81C CS 1000M MG	CS 1000E
CP IV	3521	3621	3621
CP PM	-	-	4021
CP PM Co-res CS and SS	-	-	4121
CP DC Co-res CS and SS			4221
CP MG 32 Co-res CS and SS			4321
CP MG 128 Co-res CS and SS			4421
COTS2 Co-res CS and SS			4521

Backwards/forwards compatibility

CS 1000 Release 7.0 supports COTS1 servers, however the operating system must be migrated from VxWorks to Linux and the Linux applications must be installed.

The COTS2 servers are not backwards compatible with CS 1000 Release 5.5 and older software. The COTS2 servers do not support the VxWorks operating system used in previous software releases.

The COTS2 servers are compatible with pre-CS 1000 Release 7.0 Servers when running the same software release. Depending on the applications loaded and the inter-op configuration, the total capacity of the Server may need to be lowered to that of the lowest common denominator in the cluster.

The ISP1100 Signaling Server is not supported in CS 1000 Release 7.0.

The Common Processor Dual Core (CP DC) card and the Common Processor Media Gateway (CP MG) card do not support standard or high availability configurations.

MG 1000T upgrade and migration options

The following information is intended to highlight the major considerations required to properly engineer an MG 1000T upgrade. Careful and detailed planning must be done in advance to minimize system downtime. Each option offers different levels of ease of upgrade, complexity, redundancy, long term supportability and maintenance. Select the best option according to specific customer requirements.

Option 1

Upgrade the MG 1000T to a CS 1000E and maintain it as an autonomous node

Option 1 involves upgrading the MG 1000T to a CS 1000E, using either CP PIV or CP PM Call Servers. Each existing MG 1000T chassis requires an MGC. The current PRI and media cards in the MG 1000T are maintained. The upgraded CS 1000E can still be used as a PRI gateway and contains all of the functionality of an existing CS 1000E.

Option 2 (recommended)

Migrate the functionality and PRI hardware of the MG 1000T into the CS 1000E

This option involves migrating the MG 1000T functions into a CS 1000E system. Each existing MG 1000T chassis requires an MGC. The current PRI and media cards in the MG1000T are maintained. All MG 1000T chassis are added to the CS 1000E as new MG 1000Es, and all PRI loops and DSP resources have to be added to the CS 1000E database. The NARS/BARS database on the MG 1000T must be replicated on the CS 1000E. MG 1000T Signaling Server NRS functionality can be moved to the CS 1000E node or remain as is. The NRS dialing plan must be changed accordingly.

Note 1: An MG 1000E has specific network requirements for connecting to the Call Server in terms of round trip delay and packet loss. Please see *Communication Server 1000E Planning and Engineering* (NN43041-220).

Note 2: NRS database synchronization is not supported between Signaling Servers running different releases.

Conversion and mapping information

The following information is required for the database conversion that must be performed as part of the CS 1000 Release 7.0 software installation.

Cabinet or Chassis to IPMG mapping

The following pages detail how the Small System TNs are mapped to Large System TNs. The SIPE cabinets are converted to IPMGs as shown in Table 3.

Note: Due to TN remapping, all external applications (such as Call Pilot) must to be verified following the upgrade to ensure implementation of any changes required for them to work properly with a large system TN format.

Table 3
SIPE cabinet/chassis to IPMG conversion

Cabinet/Chassis	IPMG
Call Server	000 0
Media Gateway 1	000 1
Media Gateway 2	004 0
Media Gateway 3	004 1
Media Gateway 4	008 0

Minimum software release

The conversion process can be applied to the database of existing small systems provided that the small system has a minimum software version of 23.10.

TN mapping

The following tables map the small system TNs to the CS 1000E TNs (large system TNs). The conversion feature maps the SIPE TNs to CS1000E TNs on the IPMGs.

IP phone TN mapping

When converting from small systems (Option 11C, MG1000B, CS 1000M or CS 1000S) to a CS 1000E system, the slot and unit number is mapped to the loop, shelf, card, and unit number as shown in Table 4. Because these TNs

map from a “small system” TN format to a “large system” TN format, the IP sets do NOT require reprogramming with a new TN.

Table 4
IP phone TN mapping

CS 1000S/M		CS 1000E			
Slot	Unit	Loop	Shelf	Card	Unit
61-64	0-31	96	0	1-4	0-31
65-68	0-31	100	0	1-4	0-31
69-72	0-31	104	0	1-4	0-31
73-76	0-31	108	0	1-4	0-31
77-80	0-31	112	0	1-4	0-31
81-84	0-31	96	1	1-4	0-31
85-88	0-31	100	1	1-4	0-31
89-92	0-31	104	1	1-4	0-31
93-96	0-31	108	1	1-4	0-31
97-99	0-31	112	1	1-3	0-31

ALC, DLC, analog trunk and regular IPE pack TN mapping

Table 5 provides TN mapping information for analog line cards, digital line cards, analog trunk cards, and xdrs (digital trunk cards or IP phones are not addressed in this table). Not all slots are present on all small systems.

Table 5
ALC, DLC, analog trunk and regular IPE pack TN mapping (Part 1 of 3)

CS 1000S/M		CS 1000E			
Slot	Unit	Superloop	Shelf	Card	Unit
1	0-31	0	0	1	0-31
2	0-31	0	0	2	0-31
3	0-31	0	0	3	0-31
4	0-31	0	0	4	0-31
5	0-31	0	0	5	0-31
6	0-31	0	0	6	0-31
7	0-31	0	0	7	0-31
8	0-31	0	0	8	0-31
9	0-31	0	0	9	0-31
10	0-31	0	0	10	0-31
11	0-31	0	1	1	0-31
12	0-31	0	1	2	0-31
13	0-31	0	1	3	0-31
14	0-31	0	1	4	0-31
15	0-31	0	1	5	0-31
16	0-31	0	1	6	0-31
17	0-31	0	1	7	0-31
18	0-31	0	1	8	0-31

Table 5
ALC, DLC, analog trunk and regular IPE pack TN mapping (Part 2 of 3)

CS 1000S/M		CS 1000E			
Slot	Unit	Superloop	Shelf	Card	Unit
19	0-31	0	1	9	0-31
20	0-31	0	1	10	0-31
21	0-31	4	0	1	0-31
22	0-31	4	0	2	0-31
23	0-31	4	0	3	0-31
24	0-31	4	0	4	0-31
25	0-31	4	0	5	0-31
26	0-31	4	0	6	0-31
27	0-31	4	0	7	0-31
28	0-31	4	0	8	0-31
29	0-31	4	0	9	0-31
30	0-31	4	0	10	0-31
31	0-31	4	1	1	0-31
32	0-31	4	1	2	0-31
33	0-31	4	1	3	0-31
34	0-31	4	1	4	0-31
35	0-31	4	1	5	0-31
36	0-31	4	1	6	0-31
37	0-31	4	1	7	0-31
38	0-31	4	1	8	0-31
39	0-31	4	1	9	0-31

Table 5
ALC, DLC, analog trunk and regular IPE pack TN mapping (Part 3 of 3)

CS 1000S/M		CS 1000E			
Slot	Unit	Superloop	Shelf	Card	Unit
40	0-31	4	1	10	0-31
41	0-31	8	0	1	0-31
42	0-31	8	0	2	0-31
43	0-31	8	0	3	0-31
44	0-31	8	0	4	0-31
45	0-31	8	0	5	0-31
46	0-31	8	0	6	0-31
47	0-31	8	0	7	0-31
48	0-31	8	0	8	0-31
49	0-31	8	0	9	0-31
50	0-31	8	0	10	0-31

Digital trunk mapping

This mapping (shown in Table 6) applies to DTI, DTI2, PRI, PRI2, MISIP, DPNSS and other circuit packs.

Table 6
Digital trunk mapping (Part 1 of 4)

CS 1000S/M		CS 1000E				
Slot	Channel	Digital Loop	Channel	Superloop	Shelf	Card
1	0 - 31	20	0 - 31	0	0	1
2	0 - 31	21	0 - 31	0	0	2

Table 6
Digital trunk mapping (Part 2 of 4)

CS 1000S/M		CS 1000E				
Slot	Channel	Digital Loop	Channel	Superloop	Shelf	Card
3	0 - 31	22	0 - 31	0	0	3
4	0 - 31	23	0 - 31	0	0	4
5	0 - 31	24	0 - 31	0	0	5
6	0 - 31	25	0 - 31	0	0	6
7	0 - 31	26	0 - 31	0	0	7
8	0 - 31	27	0 - 31	0	0	8
9	0 - 31	28	0 - 31	0	0	9
11	0 - 31	52	0 - 31	0	1	1
12	0 - 31	53	0 - 31	0	1	2
13	0 - 31	54	0 - 31	0	1	3
14	0 - 31	55	0 - 31	0	1	4
15	0 - 31	56	0 - 31	0	1	5
16	0 - 31	57	0 - 31	0	1	6
17	0 - 31	58	0 - 31	0	1	7
18	0 - 31	59	0 - 31	0	1	8
19	0 - 31	60	0 - 31	0	1	9
21	0 - 31	76	0 - 31	4	0	1
22	0 - 31	77	0 - 31	4	0	2
23	0 - 31	78	0 - 31	4	0	3
24	0 - 31	79	0 - 31	4	0	4

Table 6
Digital trunk mapping (Part 3 of 4)

CS 1000S/M		CS 1000E				
Slot	Channel	Digital Loop	Channel	Superloop	Shelf	Card
25	0 - 31	80	0 - 31	4	0	5
26	0 - 31	81	0 - 31	4	0	6
27	0 - 31	82	0 - 31	4	0	7
28	0-31	83	0-31	4	0	8
29	0-31	84	0-31	4	0	9
31	0-31	85	0-31	4	1	1
32	0-31	86	0-31	4	1	2
33	0-31	87	0-31	4	1	3
34	0-31	88	0-31	4	1	4
35	0-31	89	0-31	4	1	5
36	0-31	90	0-31	4	1	6
37	0-31	91	0-31	4	1	7
38	0-31	92	0-31	4	1	8
39	0-31	93	0-31	4	1	9
41	0-31	116	0-31	8	0	1
42	0-31	117	0-31	8	0	2
43	0-31	118	0-31	8	0	3
44	0-31	119	0-31	8	0	4
45	0-31	120	0-31	8	0	5
46	0-31	121	0-31	8	0	6

Table 6
Digital trunk mapping (Part 4 of 4)

CS 1000S/M		CS 1000E				
Slot	Channel	Digital Loop	Channel	Superloop	Shelf	Card
47	0-31	122	0-31	8	0	7
48	0-31	123	0-31	8	0	8
49	0-31	124	0-31	8	0	9

XNET and XPEC conversion

Although XNETs and XPECs are not configured by CS 1000 small systems, they are utilized internally by the system and appear in the database. The contents of the XNET blocks must be converted to virtual XNET blocks.

TTY conversion

Any TTYs programmed in the Call Server chassis must be moved to an equipped Media Gateway. The TTYs from small systems are converted as shown in Table 7.

Table 7
TTY conversion

TTY Port Before Conversion		TTY Port After Conversion		
Cabinet/ Chassis	Port [†]	Card	IPMG	Port
Main	0	CP PM	N/A	0
	1	MGC	000 0	1
	2	MGC	000 0	2

Table 7
TTY conversion

TTY Port Before Conversion		TTY Port After Conversion		
Cabinet/ Chassis	Port†	Card	IPMG	Port
Expansion 1	0	MGC	000 1	0
	1	MGC	000 1	1
	2	MGC	000 1	2
Expansion 2	0	MGC	004 0	0
	1	MGC	004 0	1
	2	MGC	004 0	2
Expansion 3	0	MGC	004 1	0
	1	MGC	004 1	1
	2	MGC	004 1	2
Expansion 4	0	MGC	008 0	0
	1	MGC	008 0	1
	2	MGC	008 0	2

Tone Receiver Conversion

Tone receivers are converted using the same algorithm as that used for IPE shelf conversion. The tone receivers map to cards 14 and 15 for each of the five IPMGs (see Table 8 on [page 41](#)).

Note: On CS1000S systems, any DTRs converted to Media Gateway 00 0, will need to be removed unless appropriate hardware is added. Additional DTRs will need to be programmed in the configured Media Gateways.

Table 8
Tone receiver conversion

CS 1000S/M		CS 1000E			
Slot	Unit	Superloop	Shelf	Card	Unit
0	0-7	0	0	14	0-7
0	8-11 or 8-15	0	0	15	0-3 or 0-7
If these cabinets are populated with MGCs, then these units must be configured. Unit types and unit numbers in each MG will be matched to the configuration that exists in slot 0.		0	1	14	0-7
		0	1	15	0-3 or 0-7
		4	0	14	0-7
		4	0	15	0-3 or 0-7
		4	1	14	0-7
		4	1	15	0-3 or 0-7
		8	0	14	0-7
		8	0	15	0-3 or 0-7

Conference and Tone Generator conversion

All existing Tone and Conference loops are removed and two loops (one for tone and one for conference) are allotted for each IPMG as shown in Table 9.

Table 9
Conference and Tone Generator conversion

IPMG	MG TDS	MG CONF
000 0	124	125
000 1	126	127

Table 9
Conference and Tone Generator conversion

IPMG	MG TDS	MG CONF
004 0	128	129
004 1	130	131
008 0	132	133

IPMG Configuration

The IP address for each of the IPMG must be entered in LD 97. Note that the SIPE IP addresses cannot not be used in this case since the SIPE IP connections are point to point and may not be in the same subnet as the ELAN IP address. As part of conversion the IPMG Type is set to MGC.

DSP Resources for IPMGs

Digital Signal Processor (DSP) resources must be added to Media Gateways that do not have a Voice Gateway Media Card present to provide the DSP resources required for inter-gateway calls or TDM to IP calls. You can add DSP resources to a Media Gateway with Media Gateway Controller (MGC) DSP daughterboards (DSP DB), or with a Common Processor Media Gateway (CP MG) card. Note that a Media Gateway does not require DSP resources for calls within the same Media Gateway (TDM to TDM calls). The DSP resources are required for TDM to IP calls and for calls between Media Gateways (these TDM to TDM calls use the IP network and therefore require DSP resources in each chassis). These DSP resources are only available to the Media Gateway in which the DSP is located.

Once conversion is complete, the DSP resources that were previously configured are now available to the gateway where the DSP resources are located. DSP resources are required in all gateways in order to support inter-gateway calls and TDM to IP calls. The configuration required for the new DSP resources must be performed manually, as it is not part of the conversion process.

Deleted information

The following information is removed during the conversion process:

- SIPE IP addresses (deleted from the database)
- TDS and Conference configuration
- Redundant serial port information
- Meridian Mail LSL, AML and other TNs.

Note: ACD queues are not deleted. They must be manually deleted following the conversion process.

Note: Although the above items are removed during the conversion process, the data in the compact flash remains intact with the small system database.

Campus Redundancy (High Availability) Package Support

For systems that require HA configuration, the VxWorks-based Call Server software must be deployed.

In CS 1000 Release 7.0, the Co-res CS and SS does not support an HA configuration (dual core with either Active or Inactive role). For more information see Co-resident Call Server and Signaling Server Fundamentals (NN43001-509).

Additional factors for consideration

SSC Security Device (dongle) considerations

When upgrading an existing system to Release 7.0 with a CP PM Call Server, the following actions are required:

- For SSC system conversions to CS 1000E, you must destroy or return the SSC security device to your local Nortel Repair>Returns center

- The CP PM Security Device provided with the software kit must be placed on the CP PM Call Server

IMPORTANT!

Continued use of decommissioned software is in violation of the Nortel Software Licensing Agreement and is not allowed. No further orders will be accepted for the serial number since it is decommissioned and tracked in Nortel's database. The Nortel Software Licensing Agreement details can be found in the Policy and Procedures section of the Enterprise Voice product catalogue.

NARS/BARS/Trunking Considerations

Impacts on customer trunking must be evaluated when designing and planning an upgrade. The MG 1000T is a tandem endpoint that may provide PRI PSTN access to a standalone CS 1000E and satellite locations. Each upgrade option impacts customer trunking in the following ways:

- **Option 1** - Trunking is out of service for the time it takes to upgrade and transition the Call Server, Media Gateways and Signaling Server to a CS 1000E
- **Option 2** - Trunking must be transitioned (both hardware and software) to the CS 1000E. A high level of ESN and PRI programming knowledge is required to move the trunking functions from the MG 1000T to the CS 1000E during both the planning and implementation phases of the upgrade. Typically the bulk of ESN programming is done on the MG 1000T and SPN's are used to steer PSTN calls between nodes. The NRS dialing plan entries also must be changed during the upgrade to move existing numbers associated with the MG 1000T endpoint to the CS 1000E endpoint. Special care must be taken to ensure 911 service functions as expected post-upgrade. The out of service time for the trunks vary site to site. Inbound DID/COT/TIE trunk routes could be split and cut over to the CS 1000E in a phased approach. Outbound DOD/COT/TIE trunks could be split and cutover using temporary RLIs to steer NPA, NXX and SPN calls (including 911). Tie routes that are H323/SIP can be redirected in the NRS assuming the ISM parameters have been moved to the CS 1000E and the ESN programming is in place.

Media Gateway considerations

For Options 1 and 2, each existing Media Gateway chassis in the MG 1000T must be upgraded to a MG 1000E or MG 1010. The new Media Gateway must be reprogrammed and joined to the corresponding CS 1000E node. Ethernet connections and IP configurations must be identified prior to conversion.

NRS considerations

If the Primary NRS resides within the original MG 1000T node, the NRS functionality can be moved to the CS 1000E or maintained as a standalone NRS.

NRS Servers must be upgraded to CS 1000 Release 7.0 prior to upgrading the first CS 1000 system to CS 1000 Release 7.0. The NRS must operate on the same software release as the system with the highest software release on the network.

Signaling Server considerations

If the MG 1000T is upgraded to a CS 1000E, the Signaling Servers can continue to function and are supported. If the MG 1000T is migrated to the CS 1000E the Signaling Servers can be re-deployed or used as spares.

ISP1100

ISP1100 Signaling Servers are not supported in CS 1000 Release 7.0 and must be replaced with a supported hardware platform.

CP PM BIOS requirements

The CP PM version 1 card requires BIOS Release 18 or later to be supported as a Signaling Server. The CP PM version 2 card (NTDW99CAE6) does not require a BIOS update. To upgrade the CP PM version 1 BIOS, see *Communication Server 1000E Hardware Upgrade Procedures* (NN43041-464).

ELAN, TLAN and IP considerations

If upgrading Media Gateways, the ELAN IP, TLAN IP addresses and switch ports can be re-used.

If you are replacing an SSC with a Gateway Controller, you require TLAN IP addresses and Layer 2 switch ports. If introducing a Co-res CS and SS you will need ELAN and TLAN IP addresses and Layer 2 switch ports. For more information, see *Communication Server 1000E Installation and Commissioning* (NN43041-310).

Estimating installation time

When all equipment and software is available, Nortel recommends planning a two to four hour period in which to perform the upgrade. Service interruptions can occur during this period.

System expansions and additional installations require additional time. See *Communication Server 1000E Installation and Commissioning* (NN43041-310) for details.

Making IP Peer Networking modifications also requires additional time beyond that of an upgrade. It can be performed after completing a standalone configuration upgrade. IP Peer Networking changes can involve interruption of call processing. See *IP Peer Networking Installation and Commissioning* (NN43001-313) for details.

Upgrade and installation times depend on the following criteria:

- number and availability of technicians
- familiarity with CS 1000E
- physical location of hardware components
- interoperability products (Nortel Messaging Server 500, Symposium,)
- unit testing and system testing
- unforeseen issues

Administration tools

Nortel Unified Communications Management (UCM)

The Nortel Unified Communications Management (UCM) solution provides you with an intuitive, common interface to manage and run managed elements. UCM is a container that stores several system management elements in a single repository. You have access to all network system management elements under the Unified Communications Management solution. You need to sign in only once to access the elements. A single sign-in eliminates the need for you to reauthenticate when a system management application starts.

UCM Security Services simplifies security control for managed elements and system management applications. UCM Security services manages secure access to Web applications and provides authentication and authorization with a single unified Common Service. UCM secures the delivery of essential identity and application information.

With UCM Common Services, administrators can control which users have access to specific managed elements. They can assign users to roles and map the permissions to those roles to control which operations a user can perform on an assigned managed element. Users can access only assigned elements and perform only the tasks specific to their assigned role and permissions for an element.

With UCM Common Services, the integration of managed elements within a single container provides users with centralized security, user access control, simplified management tasks, improved workflow efficiency, convenience, and time-saving advantages.

System data backup including application data

UCM can be used to back up and restore application data for Linux Base and applications. The type of data backed up is dependant on the applications running on the host server. For detailed information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

For detailed UCM information see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Element Manager

Element Manager (EM) is no longer present on a Signaling Server by default. It is no longer bundled in the Signaling Server application. You must manually select this option from UCM to deploy the EM application. Before installing or upgrading your system you must determine which Signaling Server will have Element Manager deployed.

Note: For each Call Server there must be at least 1 Signaling Server deployed with Element Manager.

Element Manager increases the speed and efficiency of system management by organizing parameters in logical groups, where single web pages provide access to information that was traditionally spread across multiple overlays. The ability of Element Manager to “hide or show information” helps the user focus on specific information, avoiding the distraction of multiple parameters.

Element Manager reduces configuration errors by providing a full text description of each parameter and acronym. It also reduces errors by simplifying parameter value selection through the use of pre-selected default values and drop-down lists.

The following management tasks can be performed using Element Manager:

- **System Status**
Enables users to perform maintenance actions on Call Server components (D-channel, MSDL, TMDI, Digital Trunk, Clock Controller, Network and Peripheral, Trunk diagnostic) and IP Telephony.
- **Configuration**
Enables users to configure customer data, trunks and routes (traditionally done in LD 14, 15, and 16), D-channel and Common Equipment data (LD 17), digital trunk interface (LD 73), Flexible Code Restriction and Incoming Digit conversion (LD 49), and the IP telephony node.
- **Network Numbering Plan**
Enables users to configure the Network Routing Service, and ESN data blocks for the Call Server (LD 86).

- **Software Upgrade**
Enables users to obtain Call Server software version, License parameters, and packages list. Users can also upgrade Voice Gateway Media Card loadware and IP Phone firmware.
- **Patching**
The existing Call Server and Voice Gateway Media Card patching still function within Element Manager, however the UCM Patching Manager provides centralized patch management to upload, install and maintain patches
- **System Utilities**
Enables users to backup and restore databases, set time and date, and upload software files and patches to a directory on the Signaling Server.

Configuration procedures for these tasks are in *Communication Server 1000E Installation and Commissioning* (NN43041-310), and *System Management* (NN43001-600).

For upgrade and configuration procedures that use Element Manager, see “Upgrading Voice Gateway Media Cards” on [page 143](#).

Network Time Protocol (NTP)

Network Time Protocol (NTP) is a feature used to synchronize local clocks across the network to a single, accurate, third-party Network Time Protocol server (typically a radio clock, atomic clock, or other Coordinated Universal Time (UTC) source).

For information on NTP configuration see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Simple Network Management Protocol (SNMP)

For information on the configuration of SNMP on Linux base see *Communication Server 1000 Fault Management — SNMP* (NN43001-719). For information on Enterprise Common Manager (ECM) and SNMP on Linux base see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Upgrading the Signaling Server

To upgrade the Signaling Server to Communication Server 1000 Release 7.0, see “Upgrading the Signaling Server” on [page 137](#).

Recorded Announcement and Music

IMPORTANT!

Currently, the CS 1000E only supports Recorded Announcement Broadcast and Music Broadcast.

H.323 Gatekeeper database migration

To migrate an H.323 Gatekeeper database to a Communication Server 1000 (CS 1000) Release 7.0 Network Routing Service (NRS) database, see *Signaling Server IP Line Application Fundamentals* (NN43001-125).

Passwords

Two login passwords are key to the upgrade process:

- 1 PWD1
- 2 Limited Access Password (LAPW)

You must configure the UCM security server to have the same usernames and passwords before you join the security domain. These passwords are only valid until you join the security domain in UCM.

PWD1

PWD1 is the central login defined at the Call Server. If the system is fully functional (that is, the connection is active) between the Call Server, Signaling Server, MG 1000E Expansions, and Voice Gateway Media Cards, the PWD1 login grants access to all Command Line Interfaces (CLIs) and Element Manager. If the link is not active, the specific login configured for each component must be used.

LAPW

Limited Access Password (LAPW) login can be configured on the Call Server to provide limited access to specified overlays. LAPWs can be used to log into the Call Server or to Element Manager. For more information, see *System Management* (NN43001-600).

First steps

Contents

This section contains information on the following topics:

Things to know	53
CS 1000 Release 7.0 product compatibility	53
Software requirements	60
Keycodes	61
What to have ready	62
Readiness checklist	63
Data checklist	62
First steps	65

Things to know

CS 1000 Release 7.0 product compatibility

Consult Table 10 for CS 1000 Release 7.0 product compatibility.

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 1 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
Management		
Element Manager	EM 7.0	

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 2 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
Enterprise Subscriber Manager	SM2.0	Will support only 2.0
Messaging		
CallPilot	5.0	Call Pilot MD'd in Oct. 2008. Only 5.0 supported.
CallPilot Mini	1.6	1.6 only MG 1000B (1.6); not on CS 1000E
Meridian Mail	Not supported	13.14 was the last release. Became EOL in Oct. 2009.
UM2000	3.3	Not supported on Option 61C/81C
HMS 400	1.1, 2.0	
Exchange UM2007	SP1	
NMC	6.0	
Attendant Console		
PC Console Interface Unit	Supported	
Meridian Attendant Console	1.2.4.11.0	
M2250 Attendant Console	Supported	
TDM Sets		
M2016S Secure Set (NA only)	Supported	
M2006	Supported	EoL Dec. 2009

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 3 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
M2008	Supported	EoL is Dec. 2009
M2216	Supported	EoL is Dec. 2009
M2616	Supported	EoL is Dec. 2009
M39xx	Supported	
IP Clients		
WLAN Handset 2210/2211	Supported	
WLAN Handset 2212	Supported	
WLAN Handset 6120/610	Supported	
WLAN IP Telephony Manager 2245	Supported	
WLAN Application Gateway 2246	Supported	
IP Phone 2004 (Phase 0)	Not supported	
IP Phone 2001 (Phase 2)	Supported	EoL Dec. 31, 2009
IP Phone 2002 (Phase 1)	Supported	EoL
IP Phone 2002 (Phase 2)	Supported	EoL Dec. 31, 2009
IP Phone 2004 (Phase 1)	Supported	EoL
IP Phone 2004 (Phase 2)	Supported	EoL Dec. 31, 2009

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 4 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
IP Phone 2007	Supported	
IP Softphone 2050 v3	Supported	
Mobile Voice Client 2050	Supported	
IP Audio-conference Phone 2033	Supported	
IP Phone 1110	Supported	
IP Phone 1120E/ 1140E	Supported	
IP Phone 1150E		
IP Phone 1120E/ 1140E (SIP)	Supported	
IP Phone 1535	Supported	
3100 Mobile Communications Client	Supported	
IP Phone 1210/1220/ 1230	Supported	
IP Softphone 3456	Supported	
AG2000	Supported	AG1000 no longer supported
Wireless		
Nortel Integrated DECT	451000, 471000 (IPE)	47000xxx on DMC8 card 45100xxx on DMC4 card Concentrated Mode only
SIP DECT	FW 4910b416	

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 5 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
Call Centre and CTI Applications		
SCCS	5.0	Not supported on MG 1000B
Meridian Link Services (MLS)	5.0	Not supported on MG 1000B
Symposium Express Call Center (SECC)	4.5	Not supported on MG 1000B
Symposium Web Center Portal (SWCP)	4.0	Not supported on MG 1000B
Contact Center	6.0, 7.0	
Nortel Remote Agent Observe	1.0	Not supported on MG 1000B
Nortel Agent Greeting	3.0	Not supported on MG 1000B
Contact Center Suite	6.0, 7.0	Not supported on MG 1000B
Periphonics IVR Applications		
ICP	1.0.1.155	Not supported on MG 1000B
Periphonics MPS 500/1000	3.0.0.15	Not supported on MG 1000B
Nortel Communication Control Toolkit (CCT) for MPS500/1000	5.0, 6.0	Not supported on MG 1000B
ACE (Agile Communication Environment)	1.1	Not supported on MG 1000B
MIXX Portfolio		

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 6 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
Integrated Call Assistant (ICA)	1.5	Not supported on MG 1000B
Integrated Conference Bridge (ICB) & ICB Professional 4.5	2.1, 3.0x, 4.0, 4.5	
Integrated Recorded Announcement (MIRAN)	3.0	
Nortel Integrated Call Director	1.0.3 & above, 2.0	Not supported on MG 1000B
Integrated Hospitality Services	1.17	
Other Call Servers		
BCM 200/ 400/ 1000	3.7, 4.0	
BCM 50	1.0, 2.0, 3.0	
BCM 450	1.0	
SRG 200/ 400	1,5	
SRG 50	3.0	
MCS 5100	4.0	
CS2000	CVM9,10,11	
CS2100	SE09,10,11	
Remotes		
Remote Office 9150, 9115, IP Adapter	1.4.2, 1.5.2, 1.6.1	Not supported on MG 1000B

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 7 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
Carrier/ Mini Carrier	7.0.3/ r11	Not supported on MG 1000B
Fiber Remote & Multi IPE Fiber	Supported	Supported in large Meridian 1 (61C/81C) and Large CS 1000M only
Line Side T1/E1	2.03	
Enhanced Line Side T1/E1	3.06	
Other Products		
SMC2450	1.1	
SR4134	4.0	
IP Trunk	3.01	
3rd Party		
Teledex	1.12.02	ND2200, LD4200, NDC2200 (DECT Cordless)
ipDialog	V 1.5.0 Build V101	SIP Tone V
Microsoft OCS2007	Wave 12, 13	
AudioCodes M2K/ M1K	5.2	
T-Metric Attendant Console	6.0	

Table 10
CS 1000 Release 7.0 CS 1000E product compatibility (Part 8 of 8)

Application	CS 1000E Release 7.0 compatibility	Notes
<p>Note 1: In addition to the systems and application compatibility chart above, information at a card and shelf level can be found in the Compatibility Section of <i>Product Compatibility</i> (NN43001-256).</p> <p>Note 2: It is possible for a Main Office Call Server and MG 1000B to temporarily run different software releases, provided the Main Office is running CS 1000 Release 7.0. This allows customers to add a single additional MG 1000B for CS 1000 Release 7.0 without having to upgrade their entire network of MG 1000Bs.</p> <p>Note 3: Mixed software configuration between a CS 1000 Release 7.0 Main Office and a CS 1000 Release 3.0 MG 1000B must be temporary.</p> <p>Note 4: Mixed software configuration between a CS 1000 Release 7.0 Main Office and a CS 1000 Release 4.0 and later MG 1000B can be indefinite.</p> <p>Note 5: In Normal mode, IP users use the feature set of the Main Office. In Local mode, IP users use the feature set of the MG 1000B. Analog or Digital users always use the feature set of the MG 1000B.</p>		

Software requirements

Table 11 lists the minimum software requirements for CS 1000 Release 7.0 software. See “Obtaining software” on [page 189](#) for information on how to obtain the latest versions of CS 1000 Release 7.0 software.

Table 11
Software requirements (Part 1 of 2)

Item	Version
Call Server	7.x
Signaling Server (see note below)	7.x
IP Line application (see note below)	7.x
IP Phone firmware (see note below)	Latest released with RIs 7.x
Firmware for Voice Gateway Media Cards	Latest released with RIs 7.x
Nortel IP Softphone 2050	Latest released with RIs 7.x

Table 11
Software requirements (Part 2 of 2)

Item	Version
Web browser	Microsoft Internet Explorer v.6.02 Java Runtime Environment (JRE) version 1.5 or higher Netscape is not supported
Note: The Signaling Server Terminal Proxy Server (TPS), IP Line 5.0 loadware, Gatekeeper, Network Routing Service, MG 1000E, Element Manager and IP Phone firmware are contained on the Signaling Server DVD.	

Keycodes

During an installation or upgrade, valid keycodes are required. A security keycode protects the installation of software, feature set (packages), License parameters, and the system ID. A security device validates the keycodes.

When upgrading a CS 1000E system to CS 1000 Release 7.0, the key code resides in a keycode file on a Compact Flash (CF) card or USB 2.0 storage device. The user is prompted to insert the CF card or storage device with the key code file.

If the entered keycode does not validate, take one of the following actions:

- Check the keycodes and make sure the correct keycodes have been entered.
- Check the software and make sure that it is the correct version for this site.
- Check the feature set and make sure the correct data has been entered.
- Check the License parameters and make sure the correct data has been entered.
- End the installation and contact your Nortel service team.

The system limits the validation of keycodes to three consecutive attempts. After the third unsuccessful attempt, the Software Installation Program returns to the main menu. Any data entered during the session is lost.

Note: If an invalid keycode is entered, the software and databases on the present system are not affected.

When the keycode validation passes, the software is installed on the system.

What to have ready

This section contains the following topics:

- “Data checklist” on [page 62](#)
- “Readiness checklist” on [page 63](#)

Data checklist

Data network planning is crucial to obtain good voice quality. For important information regarding the data and IP telephony network configuration needs, consult *Converging the Data Network with VoIP* (NN43001-260) and *IP Peer Networking: Installation and Commissioning* (NN43001-313).

The following data is required:

- **IP addresses for system components.**
Refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310) for more information.
- **IP addresses for the IP Phones.**
DHCP can be used to distribute IP addresses and network information to the IP Phones. Refer to *Signaling Server IP Line Application Fundamentals* (NN43001-125) for more detail.
- **Trunk, routing, and network zone data** (numbering plan, standard and IP trunks, Network Routing Service data).
Refer to *IP Peer Networking: Installation and Commissioning* (NN43001-313) for more detail.
- **System, telephony and voice data** (customer configuration, virtual loop and TN assignments, feature data).

Note 1: If there are BRI in the system, ensure that the **MISP and SILC/UILC** are located in the same cabinet or chassis prior to the small system to large system upgrade. The only supported configuration requires that the MISP and SILC/UILC are provisioned in the same IPMG following the upgrade.

Note 2: If there are **MFC cards** in the system, it is recommended that the MFC card reside in the same cabinet or chassis as the TDM trunk card.

Readiness checklist

As part of the upgrade process, complete the Upgrade readiness checklist.

Table 12
Upgrade readiness checklist (Part 1 of 2)

Action	✓
<p>Make sure that all the software that was ordered has been received.</p> <ul style="list-style-type: none"> • New version and patches / DEP lists • Current version • Compatibility and Planning • Ensure you can perform a direct upgrade, otherwise plot the intervening path required or have Nortel do the database conversion • If there are any external applications that have CS1000 with a Small System TN format (Card - Unit) configured as part of their interop with the CS1000 or M1 solutions, the existing TNs will map to new Large System based TNs that are in the format of SUPL- Shelf-Card-Unit. These applications may need to be changed in order to interop with the new TN that is generated as part of the conversion process. 	
Compact Flash and PCMCIA adapter for CP PIV or CP PM	

Table 12
Upgrade readiness checklist (Part 2 of 2)

Action	✓
<p>You need to ensure access to the Primary Security Server. Using an external DNS server is highly recommended to resolve FQDNs. If the external DNS server is not available you must modify the local Windows PC's host configuration in WINNT\system32\drivers\etc\hosts. If you are using a non-Windows OS for Web clients, refer to the OS documentation to configure the corresponding setup.</p> <p>For details, see <i>Unified Communications Management Common Services Fundamentals</i> (NN43001-116).</p> <ul style="list-style-type: none"> • ensure all new IPs needed are available from Network administrator • ensure all FQDNs are available from customers network administrator • ensure that the PC on the network can ping the FQDNs (or at least have the name resolve to the expected IP address, as the server may not be installed yet, but this will prove the DNS server is configured correctly) 	
<p>Prepare the network data, such as new IP addresses, as suggested in "Data checklist" on page 62 and in:</p> <ul style="list-style-type: none"> • <i>Converging the Data Network with VoIP</i> (NN43001-260) • <i>IP Peer Networking: Installation and Commissioning</i> (NN43001-313) • <i>Communication Server 1000E Installation and Commissioning</i> (NN43041-310) 	
<p>Obtain the correct keycodes for the software.</p>	

First steps

This section summarizes the steps to prepare for and initiate an upgrade to the CS 1000 Release 7.0 software.

To install new hardware in a system expansion, refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310).

As a general rule, follow the order of the chapters.

Procedure 1 Preparing for upgrade

- 1 Read the safety instructions.
- 2 Review the “Data checklist” on [page 62](#).
- 3 Complete the “Readiness checklist” on [page 63](#).
- 4 Verify compliance with system and site requirements.
- 5 Verify compliance with network requirements for system expansions (adding Media Gateways, IP Phones, new sites). Refer to *Converging the Data Network with VoIP* (NN43001-260).
- 6 Connect a serial cable from the Call Server to a maintenance terminal.
 - For a MG 1000E upgrade, connect the three-port SDI cable to DB-9 port to the back of the MG 1000E. Connect the DB-9 serial cable to connector 0.



WARNING

On the MG 1000E, do not connect a serial port to the AUX connector. It can damage the port.

- For a MG 1010 upgrade, connect a shielded CAT5 Ethernet cable from the MG 1010 Media Gateway Utility card to a NTC325AAE6 serial adapter kit. Connect a DB-9 or DB-25 serial cable from the required adapter to a maintenance terminal.

- 7 Perform a data dump.



WARNING

Both before and after an upgrade, perform a data dump on the Call Server.

LD 43 Load program

EDD Data dump

- 8 Archive the system database on the Call Server and save it to a removable media device (RMD). Label the database backup as the final data from the current software.

LD 43 Load program

BKO Copy data from primary to backup RMD

- 9 Remove all obsolete data configurations from the system.

For example, remove Meridian Mail agents, queues, and supporting network loops. Remove all EPE, RPE, TDS, MFS and conference loops (excluding XCT and IP devices).

- 10 Perform a data dump, see step 7.

- 11 Archive the system database on the Call Server and save it to an RMD, see step 8. Label the database backup as the data to be upgraded.

- 12 Upgrade the software on the system, see "Upgrading Call Server software (CP PIV, CP PM)" on [page 75](#). Use the data to be upgraded backup if you are upgrading the Call Server hardware.

- 13 Once the upgrade is complete and the system is stable, perform a data dump, see step 7.

- 14 Cold start the system (sysload) to verify that the system can reload successfully with the upgraded database.

Note: System error messages are printed during sysload if the database contains obsolete data. Perform **EDD CLR** to save the database.

End of Procedure

Co-resident Call Server and Signaling Server

Contents

Overview	67
Supported configurations	68
Co-res CS and SS upgrade paths.....	71
Hardware.....	71
Software applications	73
Element Manager	74

Overview

A Communication Server 1000 system consists of two major functional components, a Call Server and a Signaling Server. These two components have historically been running on separate Intel Pentium processor-based hardware platforms operating under the VxWorks Operating System.

The Co-resident Call Server and Signaling Server (Co-res CS and SS) runs the Call Server software, Signaling Server software, and System Management software on one hardware platform running the Linux Base Operating System. For Communication Server 1000 Release 7.0, the Co-res CS and SS is supported on various hardware platforms, see Table 1: “Hardware platform supported roles” on [page 23](#).

The Co-res CS and SS provides a cost effective solution for Communication Server 1000 system installations that do not require a high user capacity or the need for a redundant Call Server.

This chapter provides a high level overview only. For more information about Co-res CS and SS, see *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

Supported configurations

You require a Media Gateway, Gateway Controller, and Server to deploy the Co-resident Call Server and Signaling Server in the following configurations:

- Communication Server 1000E (CS 1000E)
- Branch Office Media Gateway (MG 1000B)
- Survivable Media Gateway (SMG)
- Survivable SIP Media Gateway (SSMG)
- Communication Server 1000E TDM (CS 1000E TDM)

For details on the CS 1000E TDM system, see *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

You can deploy a Co-res CS and SS as a Main Office, Branch Office, SMG or SSMG.

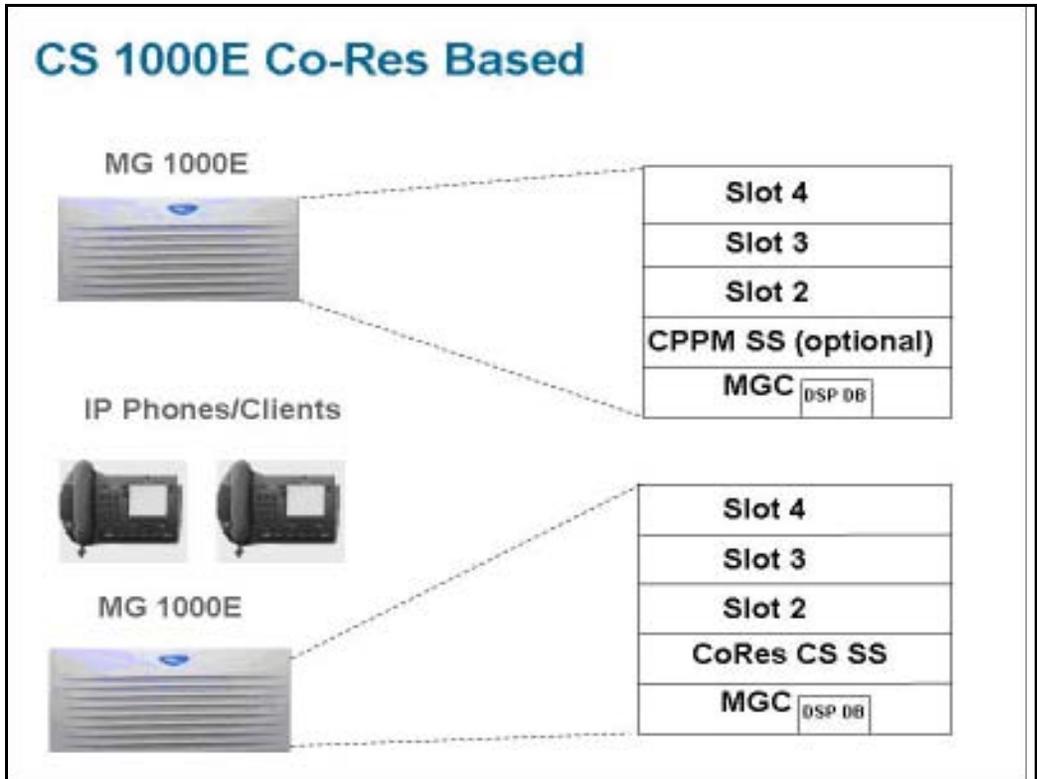
For information about installing an SMG or SSMG, see *Communication Server 1000 System Redundancy Fundamentals* (NN43001-507).

For information about CS 1000E capacity limitations, see *Communication Server 1000E Planning and Engineering* (NN43041-220).

Co-res CS and SS based CS 1000E system

Figure 2 on [page 69](#) provides an example of a CS 1000E system with a Co-res CS and SS in a MG 1000E chassis. You can also use an MG 1010, chassis, cabinet, or a COTS2 server to deploy a Co-res CS and SS.

Figure 2
CS1000E Co-res and SS system

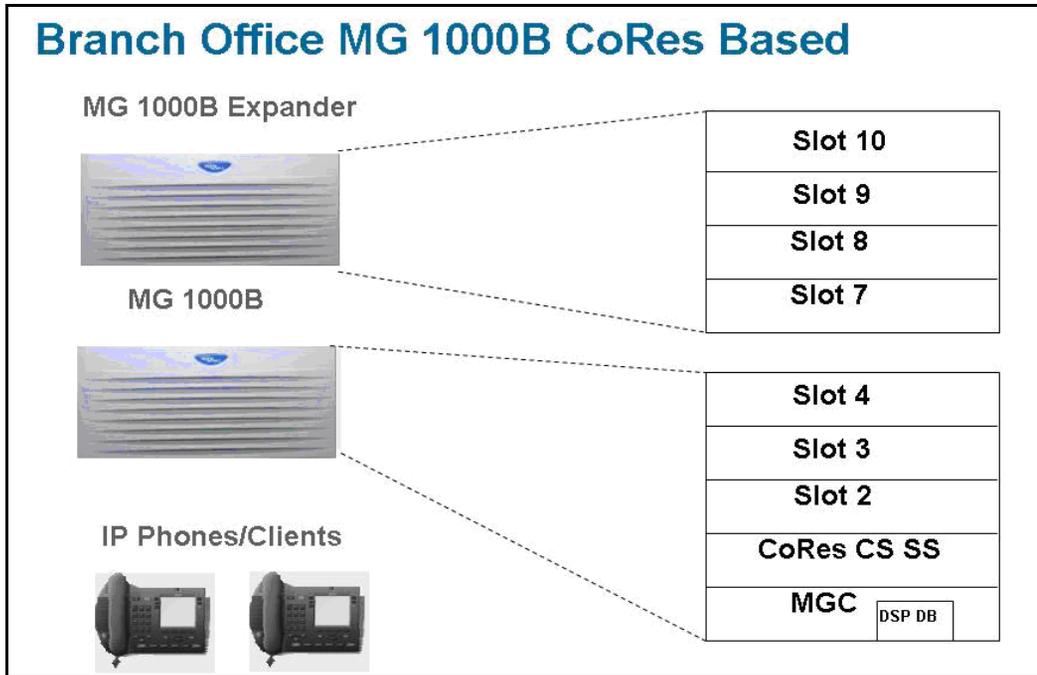


For information on adding an optional second Signaling Server to a Co-res CS and SS, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Co-res CS and SS based Branch Office Media Gateway

Figure 3 on [page 70](#) provides an example of a Co-res CS and SS based Branch Office Media Gateway (MG 1000B) system.

Figure 3
MG 1000B Co-res CS and SS system



Communication Server 1000E TDM

Communication Server 1000 Release 7.0 supports a TDM only version of the CoRes CS and SS system. The CS 1000E TDM system has the following capacity limitations:

- 800 combined TDM users (Traditional, CLASS, DECT users, including installed plus add-on)
- 5 Media Gateways
- 16 PRI cards
- 200 ACD Agents
- 0 IP Phones (no UNISlim, no SIP Line, no SIP DECT)
- 0 Virtual Trunks

The CS 1000E TDM system does not support NRS.

High Availability (HA) support

In CS 1000 Release 7.0, the Co-res CS and SS does not support an HA configuration (dual core with either Active or Inactive role). For systems that require HA configuration, you must deploy a VxWorks-based Communication Server 1000 system.

Co-res CS and SS upgrade paths

The following upgrade paths are supported for Communication Server 1000 systems.

- CS 1000 Release 6.0 or earlier Communication Server 1000E Call Server with Standard Availability (SA) to a Communication Server 1000 Release 7.0 Co-resident Call Server and Signaling Server

If you upgrade from a non-CP PM based Communication Server 1000E Call Server, you must replace your old Call Server hardware with either a CP PM card, CP MG card, CP DC card, or COTS2 server and upgrade the software.

- CS 1000 Release 6.0 or earlier Communication Server 1000E Signaling Server to Communication Server 1000 Release 7.0 Co-resident Call Server and Signaling Server
- Meridian 1 Option 11C, CS 1000M, or CS 1000S Call Server to Communication Server 1000 Release 7.0 Co-resident Call Server and Signaling Server
- Meridian 1 Option 11C Call Server to Communication Server 1000 Release 7.0 CS 1000E TDM.

The minimum CS 1000 Release for Small System migration to a Co-resident Call Server and Signaling Server is Release 23.10

Hardware

The Communication Server 1000 Release 7.0 Co-resident Call Server and Signaling Server is supported on CP PM cards, CP MG cards, CP DC cards, and COTS2 servers running the Linux Base Operating System.

The Co-res CS and SS can run on the CP PM hardware platform introduced in Communication Server 1000 Release 5.0, however the software changes from VxWorks to Linux, and a CP PM Linux upgrade kit is required. The CP PM card requires 2 GB memory, and a 40 GB hard drive to support the Co-res CS and SS configuration. CP PM version 1 cards require BIOS version 18 or higher to support the Co-res CS and SS configuration.

CP PM upgrade kit

The CP PM Signaling Server Linux Upgrade kit includes the following items:

- 2 GB Compact Flash (CF) with Linux base installation software
- 1 GB DDR SO-DIMM memory upgrade (Optional, Enterprise Configurator includes if required)
- 40 GB ATA Hard Drive (Optional, Enterprise Configurator includes if required)

CP PM media storage

The CP PM card for a Co-res CS and SS requires a 40 GB internal Fixed Media Drive (FMD). You must ensure switch S5 on the CP PM card is in position 2 to enable the system to boot from the hard drive FMD. Switch S5 in position 1 configures the CP PM card to boot from an internal Compact Flash (CF) FMD.

The CP PM card supports two types of Removable Media Drives (RMD)

- CF card, supports the installation of Linux Base and Linux applications
- USB memory stick device, supports the installation of Linux applications (cannot use to install Linux Base)

For Linux Base and Linux application software installations, the minimum size supported for the RMD is 1 GB. For more information about supported media for Co-resident Call Server and Signaling Server installations, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

CP MG, CP DC, and COTS2 media storage

The CP MG card, CP DC card, and COTS2 servers all require an internal Fixed Media Drive (FMD) loaded with the Linux Base Operating System.

The CP MG and CP DC cards support USB 2.0 storage devices as Removable Media Drives (RMD). A bootable USB 2.0 storage device can be used to install or patch the Linux Base Operating System. The COTS servers support bootable DVD. CF cards are not supported on CP MG, CP DC or COTS2 hardware.

Software applications

The Co-res CS and SS does not directly support SIP Line Gateway and SIP DECT. You must provision an additional stand-alone Signaling Server for this software.

The Co-res CS and SS supports the following software applications

- Linux Call Server
- Line Telephony Proxy Server (LTPS)
- Unicode Name Directory (UND)
- Signaling Server Gateway including H.323 Gateway and SIP Gateway
- Failsafe SIP Proxy service, Gatekeeper
- Personal Directory (PD)
- Network Routing Service (NRS)
 - You can configure the NRS as a Primary, however you can only configure NRS as a Secondary if the Primary is also running on a Co-res CS and SS.
 - The CP PM Co-res CS and SS does not support a Secondary or backup NRS to a capacity higher than the Primary NRS due to the small disk size and low call rates on a CP PM Co-res CS and SS system.
- Element Manager (EM)

- Unified Communications Management (UCM) Primary Security Server in limited deployment. For more information about UCM Primary Security Server procedures, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Element Manager

The Element Manager (EM) interface includes the configuration and enabling of Signaling Server application services such as UNISim, LTPS, SIP Gateway, H.323 Gateway, and SIP Line.

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

Upgrading Call Server software (CP PIV, CP PM)

Contents

This section contains information on the following topics::

Introduction	75
Software pre-conversion	76
Preparing for the upgrade	76
Performing the upgrade	103
Completing the upgrade	131

Introduction

This section provides instructions for a VxWorks-based local upgrade to Communication Server 1000 Release 7.0 software on a Call Processor Pentium IV (CP PIV) or Common Processor Pentium Mobile (CP PM) CS 1000E system. This NTP assumes all appropriate hardware has been upgraded according to procedures in *Communication Server 1000E Hardware Upgrade Procedures* (NN43041-464).

Have the following items available before proceeding

- Software Install Kits (see page 103)
- required Dependency list patches for the target system

A capture file should be maintained during all processes.

Software pre-conversion



IMPORTANT!

Upgrades to CS 1000 Release 7.0 are supported on Release 23 or later.

Database conversion for Meridian 1 Options 21E, 51, 61, 71, STE, NT and XT must be completed by Nortel Networks Software Conversion Lab. Consult the current Nortel Networks price book for cost and contact information.

If the system is equipped with IOP/CMDU cards the database must be converted with the Database Transfer utility.

All systems can be converted by Nortel Networks in the software conversion lab.



IMPORTANT!

Database backup information should be preserved for a minimum of 5 days.

Preparing for the upgrade

This document implements a “source- to-target” approach to performing an upgrade. It is important to correctly identify the source platform, target platform, and maintenance window required to perform the upgrade.

This chapter features check boxes indicating what condition the system should be in at that stage of the upgrade. If the system is not in the proper condition steps should be taken to correct this.

This section is written to maintain Dial Tone where possible and limit service interruptions.

Before attempting any software or hardware upgrade field personnel should follow the steps in Table 13 below:

Table 13
Prepare for upgrade steps

Procedure Step	Page
Planning	77
Upgrade Checklists	78
Preparing	78
Connecting a terminal	96
Printing site data	97
Performing a template audit	100
Backing up the database (CP PIV and CP PM data dump)	101
Performing the upgrade	103

Planning

Planning for an upgrade involves the following tasks:

- Conduct a site inspection to determine proper power and grounding.
- Review the site profile to determine proper foot space if adding new columns or modules.
- Identify all applications currently installed on the source platform.
- Identify and correct outstanding service problems.
- Verify the site log is updated with current trunking, call routing, application notes, and site contact information.
- Review all product bulletins and Nortel Alerts that impact the site.
- Prepare a contingency plan for backing out of the upgrade.

Upgrade Checklists

Upgrade checklists can be found in the “Upgrade checklists” chapter on [page 177](#). Engineers may print this section in order to facilitate the upgrade.

Preparing



IMPORTANT!

In a Campus configuration, as both cores may be physically separate, it is important to plan for required attendance at both core sites at some point in the upgrade.

Preparing for an upgrade involves the following tasks:

- Identify and become familiar with all procedures.
- Verify that all installed applications meet the minimum software requirements for the target platform.
- Determine and note current patch or Dep lists installed at the source platform.
- Determine required patch or Dep lists at the target platform for all system-patchable components (Call Server, Voice Gateway Media Cards, Signaling Servers and so on).
- Determine the required patches or DEP lists installed on all applications (CallPilot, Symposium Call Center Server, and so on).
- Determine and communicate the required maintenance window, contingency plan and the impact to the customer to complete the procedure.
- Determine if all additional LAN connections are present.
- Verify that all IP addresses and FQDNs are available. An FQDN is required for each Linux Element. Ping the FQDN to confirm it is available. If using external DNS servers (highly recommended) confirm that the DNS server resolves the FQDN to the expected IP address.
- Perform an inventory on required software and hardware.

- Secure the source software and key code.
- Secure the target software and key code.
- Verify the new key code using the DKA program.
- Print site data.

Pre-upgrade checklists

Perform the following pre-upgrade checklist procedures before upgrading a CS 1000E system.

Procedure 2 **Pre-upgrade activities**

Perform the following activities 5 to 7 days prior to the night of the software upgrade.



IMPORTANT!

Do not continue with the upgrade if any of the preupgrade checks below fails. Please contact your next level of support. Upgrade pre-checks involving system maintenance will need to be performed during the maintenance window.

- 1 Verify that you have the latest version of this document. The latest version of this document is available in “Finding the latest updates on the Nortel web site” on [page 19](#).
- 2 Verify Hardware compatibility prior to upgrade and upgrade any hardware that does not meet the minimum requirements for CS 1000 Release 7.0. Please refer to the Communication Server 1000 Release 7.0 Product Bulletin.
- 3 Verify the system meets the Memory Requirements for CS 1000 Release 7.0 as specified in the Communication Server 1000 Release 7.0 Product Bulletin.
- 4 Verify that a functioning spare CPU is available on site during upgrade.
- 5 Verify that there is a pre-tested working core modem with a direct line connected for Remote Technical Support.

- 6 Verify that all software necessary for the source and target release for all systems to be upgraded is available. Before the upgrade, check that all items on the order form are also on the packing slip. Check that all items been received. If any items are missing, contact your supplier for replacements before you begin the upgrade. See “Software Install Kits” on [page 103](#).
- 7 Review Keycode Data Sheet - (SDID, PKGS, License, TID) and ensure that you have all the necessary Keycodes for both the source and target software. See “Keycodes” on [page 61](#).
- 8 Verify that system is patched current for all patchable elements on the system using the "Upgrades" - Meridian ISSP Report and Conflict Checker (MIRCC) Tool, paste in an ISSP (MDP ISSP) Output and get a Detailed Patch Report.

Note 1: Upgrades MIRCC TOOL is available via Enterprise Solutions Patch Library (ESPL): <http://www.nortel.com/espl>. **Access to the Enterprise Solutions Patch Library requires a Distributor account and password.**.Once logged onto ESPL, go to: "Upgrades" - Meridian ISSP Report and Conflict Checker (MIRCC).

Note 2: Please refer to Bulletin: 2006007126 available on the Nortel Technical Support Portal for further details on the use of the Upgrades MIRCC Tool. Apply any missing Patches and remove any Obsolete Patches.

- 9 Verify that all required patches at the target platform (Release 6.0) as generated by the Upgrades MIRCC for all system-patchable components (Call Server, Voice Gateway Media Cards, Signaling Servers and so on) are available on site.
- 10 Print Site Data – See “Printing site data” on page 65.
- 11 Perform a Template Audit - See“Performing a template audit” on page 68.
- 12 Perform midnight test routines and ensure any errors addressed prior to upgrade. Verify that 5 days prior to the upgrade there are not:
 - a. Any type of system triggered restart (Warm, Cold, or Sysload).
 - b. Swd watchdog timeouts (e.g. BUG7058 SWD: Swd watchdog timer expired on task tSL1).
 - c. Semtake memory issues (e.g. BUG0584 SeaWeed memory library semTake failed memory).
 - d. Hardware Watchdog Interrupts (e.g.BUG7060 SWD: HARDWARE WATCHDOG INTERRUPT EVENT).

- e. Disk Cache Errors (e.g. 0x22bb3dd8 (tSysPhase1): disk cache error: device 371ab80 block 1279235 errno c0003, disk read failed).
- f. ELAN issues (e.g. ELAN009 ELAN 0 host IP=10.60.78.4 disabled, write to socket fail due to far end disconnect or Ethernet problems, ELAN0028 The following server failed to register it's pbxLink).
- g. Hardware Diag Failures (e.g. DIAG0002 Diagnostic: Faulty Hardware watchdog diag).
- h. IP Link Failures to MGCs (e.g. SRPT0016 OMM: IP link is DOWN between Call Server and Media Gateway, GC0018 MGC ELAN heart-beat connection to Call Server is down. Switching to alternate - port number, SRPT0016 OMM: IP link is DOWN between Alternate Call Server 1 and IPMG[0 0]).
- i. QoS errors (e.g. QOS0019 QoS unacceptable packet loss: [98.5] % in zone [1]).
- j. CMDU Failures (e.g. BUG7339 ROM OS 0: ERROR "CMDU VOL Init". Restarting with code: 52).

If you encounter any of the above errors or failures, contact your next level of support to ensure that these problems are resolved prior to any upgrade activity.

- 13** Enable System monitoring tool (AHST) in Overlay 22. This task will collect the following system outputs (they are not enabled by default):
 - Configuration changes
 - Alarms reports (AUD, SSH)
 - Error reports
 - BUG captures
- 14** Enter STAT LOOP X commands in Overlay 32 to ensure system physical and Virtual TNS are idle:
 - Enter STAT command in Overlay 60 to get status of all loops to ensure what loops are idle.
 - Enter ssck 0 and 1 for status of system clocks.
 - Enter lcnt for status of span errors.
 - Enter STAT DCH command in Overlay 96 to get status of of DCH channels to ensure they are active.

- Enter STAT ELNKcommand in Overlay 137 to get status of ELNK to ensure ELNK is link is up.

For details see *Software Input Output Reference - Maintenance* (NN43001-711).

15 Test the System Utility card.

LD 135	Load program
STAT CPU	Get the status of the System Utility card
STAT CNI	Test the System Utility card
STAT HEALTH	Display the Call Server health count status

16 Print the history file.

LD 17	
REQ	PRT
TYPE	ADAN
ADAN	NEW HST
SIZE	(0)–65534
USER	When ADAN = HST, users can be BUG, MCT, MTC, SCH and TRF.

17 Prior to System Upgrade, make two current backups to external media:

LD 43	Load program
BKO	Copy data from primary to backup device

18 Nortel recommends you to have two bootable removable media devices (RMD) for site upgrades. See “Making a bootable RMD” on [page 87](#).

19 Perform a sysload and verify no abnormal messages appear before the upgrade.

End of Procedure

Pre-upgrade checklists for Geographic Redundant Survivable sites

If you have a system with a Geographic Redundant (GR) Primary site and N-way Survivable Secondary sites, Nortel recommends you to upgrade the Survivable Secondary sites before upgrading the Primary site. For more information on GR systems, see *System Redundancy Fundamentals* (NN43001-507).

A typical Survivable Secondary site contains the following components:

- Gateway Controller with DSP resources in a Media Gateway
- IPE equipment (Line and Trunk cards) in a Media Gateway
- Media Cards in a Media Gateway
- Survivable Servers

The applications running on a Survivable Server can include Call Server (equipped with GR Secondary Server package), Terminal Proxy Server (TPS), Virtual Trunk (Vtrk), Element Manager (EM), and failsafe Network Routing Service (NRS).

During a Survivable site upgrade, your focus is to upgrade the software running on the Survivable Servers. Before you begin upgrading the Survivable Server software, you must prepare the network and equipment.

The following lists describes the pre-upgrade activities required during a GR Survivable site upgrade.

- The Unified Communication Manager (UCM) Primary and Backup Servers in the CS 1000E network must be upgraded to the latest CS 1000 software.
 - UCM member Servers running a previous software release are supported.
 - UCM member Servers running a newer software release than the UCM Primary and Backup Servers are not supported.
- The Network Routing Service (NRS) Primary and Secondary Servers in the CS 1000E network must be upgraded to the latest CS 1000 software.

- Failsafe NRS Servers running a previous software release are supported.
- Failsafe NRS Servers running a newer software release than the NRS Primary Server are not supported.
- All Gateway Controllers must be upgraded to the latest CS 1000 software release loadware. The Gateway Controller loadware is provided by the Call Server software.
 - Gateway Controller software is backwards compatible with previous CS 1000 Call Server software.
 - Gateway Controllers running older loadware than the CS 1000 Call Server are not supported.
- All Media Cards must be upgraded to Release 6.0 or newer software.
 - Media Cards running Release 5.5 and older software are not supported.
- Digital telephone and peripheral equipment must be running the same software release as the Call Server.
 - The Call Server software can automatically upgrade TMDI card loadware.
 - Other card loadwares are not automatically upgraded.
- IP Phone firmware must be upgraded.
 - The IP Phone firmware is bundled in the Signaling Server TPS application.
 - The firmware is upgraded automatically if the TPS detects an older version running on an IP Phone.

Perform the following procedure to prepare the system for a Secondary site upgrade.

Procedure 3**Pre-upgrade activities for GR Survivable sites**

- 1 Remove all IP Phone firmware on the TPS Servers at the Secondary sites.

Note: You must perform IP Phone firmware upgrades from the TPS Servers at the Primary site.

- 2 Disable the automatic Gateway Controller upgrade option on the Secondary Call Servers.

LD 143 Load program

DIS AUTOUPGMG Disable Gateway Controller auto upgrades

- 3 Ensure all IP Phones are running the latest firmware. If new firmware is available, upgrade the firmware from the TPS Primary site. For IP Phone firmware upgrade procedures, see *Signaling Server IP Line Application Fundamentals* (NN43001-125).
- 4 Ensure all digital telephones and TMDI packs are running the latest PSDL firmware. If new PSDL firmware is available, install the new firmware on the Primary Call Server. Upgrade the digital telephones and TMDI packs with the new firmware.
- 5 Ensure the Gateway Controllers are running the latest loadware. If new MGC loadware is available, upgrade the Gateway Controller from the Primary Call Server.

End of Procedure

Once the pre-upgrade preparation is complete, perform the network wide upgrade for a GR Survivable system.

Procedure 4**Upgrading a GR Survivable system**

- 1 Upgrade the UCM Primary and Backup Servers.
- 2 Upgrade the NRS Primary and Secondary Servers.
- 3 Upgrade the Survivable Servers at the GR Secondary sites.
 - Backup all data and upgrade the Servers at each Secondary site. See “Performing the upgrade” on [page 103](#), and *Signaling Server IP Line Application Fundamentals* (NN43001-125).

- For Co-resident Call Server and Signaling Servers at Secondary sites, upgrade the GR Secondary Call Server first. Proceed with upgrading the remaining Linux-based Servers, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
 - During the GR Secondary Call Server upgrade, Nortel recommends you disable the Gateway Controller automatic upgrade option.
- 4 Ensure the Survivable Servers upgraded successfully and that the database converted successfully.
 - 5 Once all Secondary site Server upgrades are complete, proceed with upgrading the Servers at the Primary site.

End of Procedure

If you performed all the GR Secondary site checks and procedures, and the upgraded Survivable Servers are called into service (WAN outage) before you complete the Primary Server upgrades, the following events occur:

- The Gateway Controllers successfully register to the GR Secondary Call Server. The Gateway Controllers are running the latest loadware, and the MGC automatic upgrade option is disabled on the Secondary Call Server.
- The Media Cards successfully register to the GR Secondary Call Server. The Media Cards are running Release 6.0 or newer software.
- The IP Phones successfully register with the TPS application on the Survivable Signaling Server. No firmware upgrades are necessary since the IP Phones are currently running the latest firmware.
- The digital telephones and TMDI cards are operational once the Gateway Controller registers to the Secondary Call Server. No firmware upgrades are necessary since the digital telephones and TMDI cards are currently running the latest firmware.
- The Virtual Trunk Gateway and the Failsafe NRS on the Survivable Server route SIP trunk calls.

Once service is restored to the Primary site (WAN connection online), the following events occur:

- The Gateway Controllers successfully re-register to the GR Primary Call Server.
- The Media Cards successfully re-register to the GR Primary Call Server.
- The IP Phones successfully re-register with the TPS application on the Primary Signaling Server.
- The digital telephones and TMDI cards are operational once the Gateway Controller re-registers to the Primary Call Server.
- The Virtual Trunk Gateway at the Primary site and the Primary NRS route SIP trunk calls.

Making a bootable RMD

The 1 GB installation CF card ships pre-formatted and bootable from Nortel. If the Nortel CF card does not boot, you can make it bootable by performing Procedure 5 on [page 88](#).

Note: Nortel 512 MB CF cards are not supported. Nortel does not provide technical support for customer provided CF cards.

For VxWorks based CP PIV and CP PM cards, 1 GB or larger CF cards are supported as the bootable RMD. USB devices are not supported.

Perform the following procedure to create a bootable Call Server software CF card.



CAUTION — Data Loss

The PC utility used in the following procedure (mkbootrmd.bat) does not validate whether the drive letter entered is a valid RMD. You must enter the correct drive letter when prompted or risk formatting the incorrect drive.

Note: This utility is supported by all versions of Microsoft Windows.

Procedure 5

Creating a bootable Call Server software CF card

- 1 Download the latest software load zip file for your platform type (CP PIV, CP PM) from the Nortel website to a folder on your PC.
- 2 Navigate to the folder on your PC where you downloaded the file.
- 3 Extract all files to a temporary folder. Unzip the Call Server software load zip file to create the following six directories:
 - \backup
 - \install
 - \keycode
 - \licenses
 - \swload
 - \utilities
- 4 Insert the CF card into the PC.



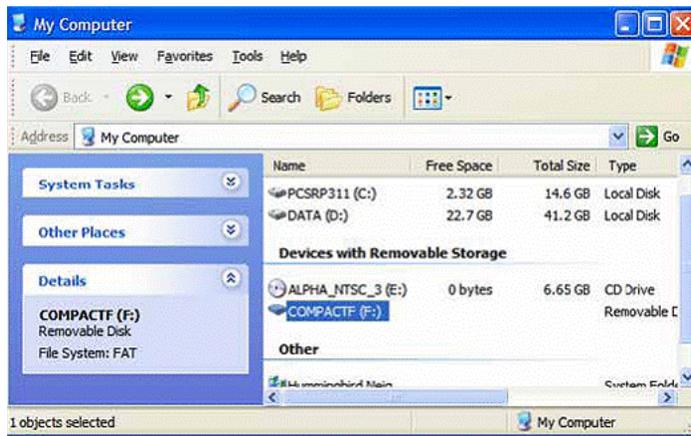
IMPORTANT!

The CF card must be 1 GB.

- 5 Click on **My Computer** icon to verify the drive letter assigned to the CF drive, see Figure 4 on page 89.

In this example, the CF card is assigned to drive letter F.

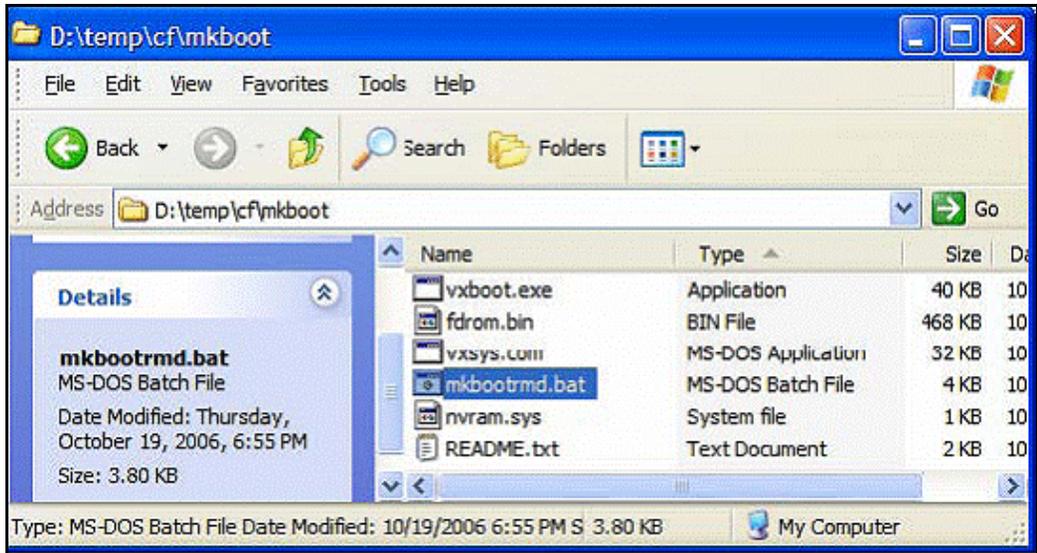
Figure 4
Verify CF card drive letter



- 6 Navigate to the folder on your local PC where you unzipped the Call Server software load files.
- 7 Open the Utilities directory and locate the *mkbootrmd.bat* file, see Figure 5 on page 90.

The *mkbootrmd* batch file can format the CF card and make the CF card bootable.

Figure 5
mkbootrmd.bat folder



- 8 Double click the mkbootrmd.bat file to start the application.

The warning screen is shown, see Figure 6 on [page 91](#). Press any key to continue.

Figure 6
mkbootrmd.bat

```
C:\WINDOWS\system32\cmd.exe
mkbootrmd.bat
-----
*****
                WARNING:
                -----
* -----
* THIS UTILITY FORMATS THE RMD
* THE DATA ON THE CARD WILL BE ERASED....!
* -----
* This utility creates Bootable RMD for CS 1000M and CS 1000E,
  which can be used to boot a system with CPPIU or CPPM processor
* This utility assumes that the drive entered is correct.
  So, please enter the correct RMD drive.
* For more information please read README_BOOTABLE_RMD.txt
*****
Please insert a RMD (Compact Flash) in drive now.
Press any key to continue . . . _
```

- 9 Enter the drive letter of your RMD, see Figure 7 on [page 92](#). Use the CF card drive letter assigned from your PC that you verified in step 5.

	IMPORTANT!
The <i>mkbootrmd.bat</i> file does not verify the drive assignment. It is possible to format other drives on the PC or Laptop.	

Figure 7
mkbootrmd.bat RMD selection

```
C:\WINDOWS\system32\cmd.exe
WARNING:
-----
* -----
* THIS UTILITY FORMATS THE RMD
* THE DATA ON THE CARD WILL BE ERASED....!
* -----
* This utility creates Bootable RMD for CS 1000M and CS 1000E,
  which can be used to boot a system with CPPIU or CPPM processo
* This utility assumes that the drive entered is correct.
  So, please enter the correct RMD drive.
* For more information please read README_BOOTABLE_RMD.txt
*
*****
. Please insert a RMD (Compact Flash) in drive now.
Press any key to continue . . .
Please enter the Drive letter of your RMD:e
.
Insert new disk for drive E:
and press ENTER when ready...
```

- 10 Press **Enter** to format and create a bootable Call Server CF card. The CF card formats and the system copies files, see Figure 8 on [page 93](#).

Figure 8
mkbootrmd.bat creation

A screenshot of a Windows command prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe". The command prompt shows the output of the mkbootrmd.bat command. The text displayed is: 16,384 bytes in each allocation unit. 62,233 allocation units available on disk. 16 bits in each FAT entry. Volume Serial Number is FCD5-4F6A . RMD format Successful Installing Boot sector Copying files bootrom.sys copied OK. . Check whether the following output shows . "All the specified file(s) are contiguous" . * * * WARNING * * * .IF THE FILES ARE NOT CONTIGUOUS, . PLEASE RECREATE THE RMD . * * * * * . Press any key to continue

- 11 The boot sector files (bootrom.sys and nvram.sys) are copied making the RMD bootable. Press any key to continue, see Figure 9 on [page 94](#).

Figure 9
mkbootrmd.bat confirmation

```
C:\WINDOWS\system32\cmd.exe
. Check whether the following output shows
. "All the specified file(s) are contiguous"
.
.      * * * WARNING * * *
. IF THE FILES ARE NOT CONTIGUOUS,
. PLEASE RECREATE THE RMD
.      * * * * *
. Press any key to continue . . .
The type of the file system is FAT.
Volume CS1000BOOT created 3/25/2010 1:30 PM
Volume Serial Number is FCD5-4F6A
Windows is verifying files and folders...
File and folder verification is complete.
Windows has checked the file system and found no problems.

1,019,625,472 bytes total disk space.
    524,288 bytes in 1 files.
1,019,101,184 bytes available on disk.

    16,384 bytes in each allocation unit.
    62,233 total allocation units on disk.
    62,201 allocation units available on disk.
All specified files are contiguous.
.
Press any key to continue . . .
```

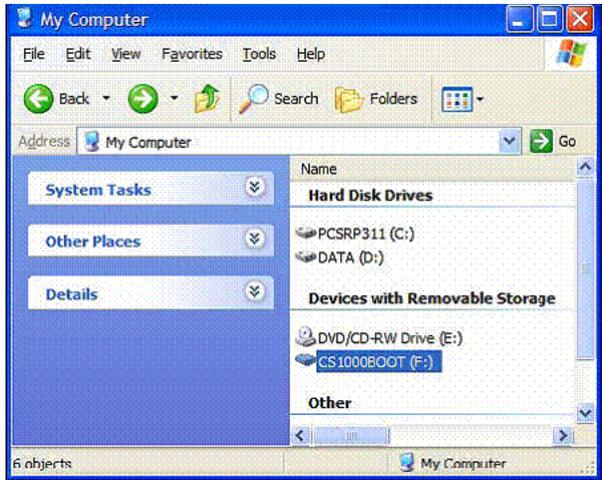
- 12 Verify the following message is shown:
"All the specified files are contiguous".

If this message is not shown, repeat this procedure starting from step 8.

Note: This message indicates that the RMD formatting process is successful and the CF card is now ready to load the Call Server software and system components..

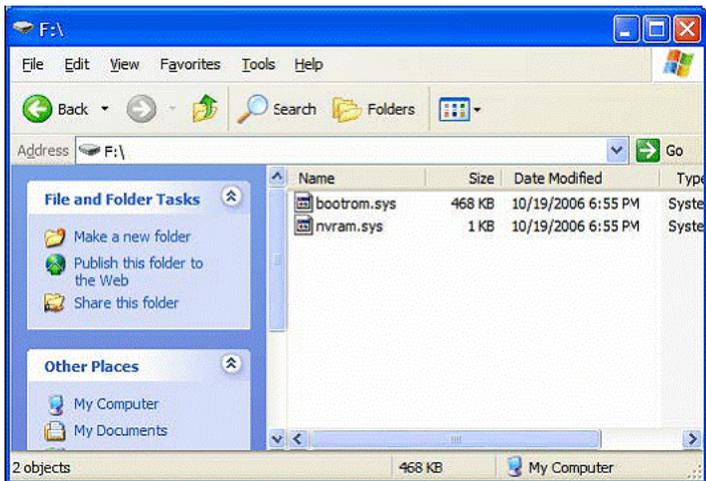
- 13 Press any key to close the mkbootrmd.bat program.
- 14 Click **My Computer** to verify the CF drive is renamed to CS1000BOOT, see Figure 10 on [page 95](#).

Figure 10
CS1000BOOT drive name



- 15 Double-click the CF drive to verify that it contains the *bootrom.sys* and *nvrnm.sys* files, see Figure 11 on page 95.

Figure 11
CF card boot files



16 Navigate the folder on your PC that contains the Call Server software load folders and files.

17 Copy all the folders to the CF card.

Note: This can take up to 12 minutes depending on the speed of the computer. The files are copied from the hard drive on the local PC to the CF card in the CF drive.

When all subfolders and files are copied successfully to the CF card, it can be used to install or upgrade the software on a Call Server.

18 Remove the CF card from the CF drive and label it appropriately.

An example for a label is, Call Processor, CS-x.xx.xx, where x.xx.xx represents the Call Server software version.

End of Procedure

Connecting a terminal

Procedure 6 **Connecting a terminal**

A maintenance terminal is required to access the Call Servers during the upgrade procedure.

1 Connect a terminal to the COM 1 port on the faceplate of the CP PIV card or the Serial Port 0 on the CP PM card of the Call Server.

Note: In case of HA, connect to inactive Call Server.

2 The settings for the terminal are:

a. Terminal type: VT100

b. 9600 Baud

c. Data bits: 8

- d. Parity: N
- e. Stop bits: 1
- f. Flow control: none

End of Procedure

Printing site data

Print site data to preserve a record of the system configuration (Table 14 on [page 97](#)). Verify that all information is correct. Make corrections as necessary.

Note: Items marked with an asterisk (*) are required. Other items are recommended for a total system status.

Table 14
Print site data (Part 1 of 4)

Site data	Print command	
Terminal blocks for all TNs	LD 20	
	REQ	PRT
	TYPE	TNB
	TN	<cr>
	CDEN	<cr>
	CUST	<cr>
	DATE	<cr>
	PAGE	<cr>
DES	<cr>	
Directory Numbers	LD 20	
	REQ	PRT
	TYPE	DNB
	CUST	<cr>

Table 14
Print site data (Part 2 of 4)

Site data	Print command	
Attendant Console data block for all customers	LD 20	LD 20
	REQ	PRT
	TYPE	ATT, 2250
	CUST	<cr>
*Customer data block for all customers	LD 21	LD 21
	REQ	PRT
	TYPE	CDB
	CUST	<cr>
Route data block for all customers	LD 21	
	REQ	PRT
	TYPE	RDB
	CUST	Customer number
	ROUT	<cr>
	ACOD	<cr>
*Configuration Record	LD 22	
	REQ	PRT
	TYPE	CFN
*Software packages	LD 22	
	REQ	PRT
	TYPE	PKG
*Software issue	LD 22	
	REQ	ISS
Tape ID	LD 22	
	REQ	TID

Table 14
Print site data (Part 3 of 4)

Site data	Print command	
* Peripheral software versions	LD 22	
	REQ	PRT
	TYPE	PSWV
	LD 22	
Used and unused ISM parameters.	REQ	PRT
	TYPE	SLT
ACD data block for all customers	LD 23	
	REQ	PRT
	TYPE	ACD
	CUST	Customer Number
	ACDN	ACD DN (or <CR>)
Multi-purpose ISDN Signaling Processor (MISP) card	LD 27	
	REQ	PRT
	TYPE	MISP
	LOOP	loop number (0-158)
	APPL	<cr>
	PH	<cr>
DTI/PRI data block for all customers	LD 73	
	REQ	PRT
	TYPE	DDB
Print the configured host information	LD 117	PRT HOST (provides system IP addresses)

Table 14
Print site data (Part 4 of 4)

Site data	Print command
Superloops and XPEs	LD 97 REQ CHG TYPE SUPL SUPL Vxxx V stands for a virtual superloop and xxx is the number of the virtual superloop. xxx = 0-252 in multiples of four for MG 1000E xxx = 96-112 in multiples of four for MG 1000T (See Table 29)
<p>Note: Items marked with asterisks (*) are required printout for conversion. Other items are recommended for a total system status.</p>	

Performing a template audit

A template audit (LD 01) reviews the templates in your system. Corrupted and duplicate templates are cleaned up. An example of the information generated during the audit is listed below.

Note: The template audit may take an extended period of time on large systems. Run the audit during a low traffic period.



CAUTION

Loss of Data

Do not abort this overlay until the audit is complete. If the overlay is interrupted, data will be corrupted.

LD 01 The audit begins as soon as LD 01 is entered.

CONFIRM TEMPLATE AUDIT NOW? (Y/N) Y

STARTING PBX TEMPLATE SCAN

STARTING SL1 TEMPLATE SCAN

TEMPLATE 0001 USER COUNT OK CHECKSUM OK

TEMPLATE 0002 USER COUNT OK CHECKSUM OK

Backing up the database (CP PIV and CP PM data dump)

Procedure 7

Performing a data dump to backup the customer database:

- 1 Log into the system.
- 2 Insert a CF card into the active Core/Net RMD slot to back up the database.
- 3 Load the Equipment Data Dump Program (LD 43). At the prompt, enter:

LD 43 Load program.

. EDD

- 4 When "EDD000" appears on the terminal, enter:

EDD Begin the data dump.



CAUTION — Service Interruption

Loss of Data

If the data dump is not successful, do not continue; contact your technical support organization. A data dump problem must be corrected before proceeding.

- 5 When "DATADUMP COMPLETE" and "DATABASE BACKUP COMPLETE" will appear once the data dump is complete.

**** Exit program

- 6 The message "Backup process to local Removable Media Device ended successfully" appears. Remove and label the CF card.

End of Procedure

Performing the upgrade

Reviewing upgrade requirements

**WARNING**
Loss of Data

CP PM VxWorks systems do not require a BIOS upgrade for CS 1000 Release 7.0. A BIOS upgrade can be required for CP PM cards deployed as a Linux based Signaling Server for CS 1000 Release 7.0.

This section describes the *minimum* software required for CS 1000 Release 7.0. Verify that *all* software has been received.

Before the upgrade, check that items on the order form are also on the packing slip. Check that all items been received. If any items are missing, contact your supplier for replacements before you begin the upgrade.

**WARNING**
Service Interruption

DO NOT proceed with the upgrade if any of the required items are missing. All items must be received to complete the upgrade.

Software Install Kits

The Software Install Kits are generic sets of software and utility programs that are specific to a single release and issue of software. Obtain a new kit when upgrading to a new release or issue of software.

Table 15 lists the contents of the Software Install Kits for CP PIV and CP PM.

Table 15
Contents of the Software Install Kits

CP PIV Compact Flash Software Install Kit (NTE907YBE5)		
Item	Quantity	Description
CF card (512 MByte)	1	A CF card containing the Install Software files, CS 1000 Release 7.0 software, Dep. Lists (PEPs), and the keycode file.
CF card (128 MByte)	1	Blank for backup
Documentation CD-ROM	1	Nortel CS 1000 Release 7.0 Documentation CD
CP PM Compact Flash Software Install Kit (NTM442CD)		
CF card (512 MByte)	1	A CF card containing the Install Software files, CS 1000 Release 7.0 software, Dep. Lists (PEPs), and the keycode file. This applies to VXworks systems only.
CF card (128 MByte)	1	Blank for backup
CF card (1 GByte)	1	Blank for CP PM card
Documentation CD-ROM	1	Nortel CS 1000 Release 7.0 Documentation CD

Splitting the Call Servers

Note: Procedure 8 on [page 105](#) and Procedure 9 on [page 106](#) are not applicable to a CS 1000E SA system.

Procedure 8**Checking that Call Server 0 is active**

To upgrade Call Server 1, verify that Call Server 0 is the active side performing call processing:

- 1 Verify that Call Server 0 is active.

LD 135 Load program

STAT CPU Get the status of the CPUs

- 2 If Core 1 is active, make Core 0 active:

SCPU Switch to Call Server 0 (if necessary)

******** Exit program

- 3 Stat Health of the CPU and memory:

LD 135

STAT HEALTH Get status of CPU and memory

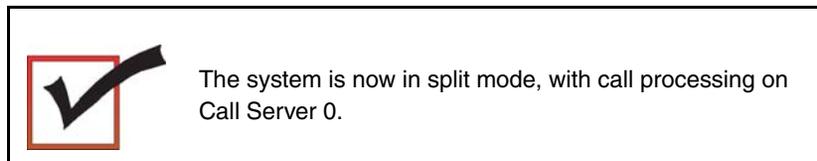
******** Exit the program

Note: If there is a health mismatch, take steps to correct the issue, including contacting Nortel Technical Support, before proceeding with the upgrade.

Procedure 9
Splitting the Call Servers

1 In Call Server 0, enter the SPLIT command from LD 135.

LD 135	Load program
SPLIT	Split the Call Servers
****	Exit program



Upgrading to CS 1000E Release 7.0 (CP PIV or CP PM)

Upgrading the software

Perform Procedure 10 to upgrade CP PIV or CP PM systems to CS 1000E Release 7.0

If upgrading a CS 1000E HA system:

- Call Servers must be split before the upgrade, see Procedure 9
- Upon completion of the Call Server 1 upgrade, you must perform the procedure again and upgrade Call Server 0. Following the upgrades, the Call Servers must be joined.

Procedure 10

Upgrading the software (CP PIV or CP PM)

- 1 Check that a terminal is connected to COM 1 port in Call Server 1 (inactive core). The settings for the terminal are:
 - a. Terminal type: VT100
 - b. 9600 Baud
 - c. Data bits: 8

- d. Parity: N
 - e. Stop bits: 1
 - f. Flow control: none
- 2 Insert the installation software RMD into the CF card slot on Call Server 1 (inactive core).
 - 3 Perform a KDIF in LD 143. See Table 22 on [page 181](#).
 - 4 Press the manual RESET button on the Call Server 1 (inactive core) card faceplate.
 - 5 Press **F** to force board to boot from faceplate drive.
 - 6 During SYSLOAD, the following prompt appears:

```

Read boot parameters from:

F: Faceplate compact flash
H: Hard Drive

0 [H]
    
```

Press **F** to boot from the compact flash (which contains the software).

- 7 Press **<CR>** at the initial Install Tool screen.

```

Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
-----
                                     NORTEL
                                     Communication Server 1000 Software
                                     Install Tool version 39
                                     Copyright 1992 - 2007

Please press <CR> when ready ...
    
```

- 8 Observe the following PE/EPE and PDT password warnings. Following each warning, press **y** or **<CR>** to proceed

```
WARNING:

This software does not support TNs
configured on PE/EPE shelves. Upgrading to
this software release will permanently
disable all TNs configured on PE/EPE and
will not allow new TNs to be configured.

Proceed with the upgrade? (Y/N) y

WARNING:

Upgrading from pre-Release 4.5 software to
Release 4.5 or higher will result in the
system PDT passwords being reset to default.

Proceed with the upgrade? (Y/N) y
```

- 9 Press **u** or **<CR>** at the Main Menu to enter the install menu (keycode authorization).

```
          M A I N   M E N U

The Software Installation Tool will install or
upgrade Communication Server 1000 Software,
Database and the CP-BOOTROM. You will be
prompted throughout the installation and given
the opportunity to quit at any time.

Please enter:

<CR> -> <u> - To Install menu
        <t> - To Tools menu.
        <q> - Quit.

Enter Choice> <u>
```

The system searches for available keycode files in the "keycode" directory on the RMD.

- 10** The system displays the keycode file(s) available, see the following example Select the keycode you require on the system.:

```
The following keycode files are available on the
removable media:
```

```

Name                               Size   Date       Time
-----
<CR> -> <1> -keycode.kcd 1114 mon-d-year hr:min
<2> - KCport60430m.kcd   1114 mon-d-year hr:min
<q> - Quit
Enter choice> 2
```

Note: A maximum of 20 keycode files can be stored under the “keycode” directory on the RMD. The keycode files must have the same extension “.kcd”.

The system validates the selected keycode and displays the software release and machine type authorized.

```
Validating keycode ...
Copying "/cf2/keycode/KCport60430m.kcd" to "/u/
keycode" -
Copy OK: 1114 bytes copied

The provided keycode authorizes the install of
xxxx software (all subissues) for machine type
xxxx (CP xx processor on <system>).
```

- 11 The software release displayed depends on the keycode file content. The system requests keycode validation Press **y** or **<CR>** to confirm and continue to the next step, or press **n** to select a different keycode..

```
Communication Server 1000 Software/Database/  
BOOTROM RMD Install Tool  
  
=====
```

Please confirm that this keycode matches the
System S/W on the RMD.

Please enter:

 <CR> -> <y> - Yes, the keycode matches.
Go on to Install Menu.

 <n> - No, the keycode does not match.
Try another keycode.

Enter choice>

- 12 The system displays the Install Menu. Press **a** or **<CR>**.

Note: Option A uses the existing database on the FMD. Option B allows you to install a pre-configured database from a CF card..

```
Communication Server 1000 Software/Database/  
BOOTROM RMD Install Tool  
=====
```

I N S T A L L M E N U

The Software Installation Tool will install or upgrade Communication Server 1000 Software, Database and the CP-BOOTROM. You will be prompted throughout the installation and given the opportunity to quit at any time.

Please enter:

<CR> -> <a> - To install Software, CP-BOOTROM.
 - To install Software, Database, CP-BOOTROM.
<c> - To install Database only.
<d> - To install CP-BOOTROM only.
<t> - To go to the Tools menu.
<k> - To install Keycode only.

For Feature Expansion, use OVL143.

<p> - To install 3900 set Languages.
<q> - Quit.

Enter Choice> <a>

13 Perform this step for CP PM only. Confirm the CP PM side location.

```
Communication Server 1000 Software/Database/  
BOOTROM RMD Install Tool  
  
=====
```

This CS 1000 Call Processor is set to side 0

Please confirm that the side information is correct.

Please enter:

<CR> -> <y> - Yes, the side information is correct.

 <n> - No, the side information is incorrect. Go on to Side Setting Menu.

Enter choice> <CR>

- i. Press **y** or **<CR>** to confirm correct CP PM side location.
- OR
- ii. Press **n** to configure side setting for CP PM card.

14 Perform this step for CP PM only. Confirm IPMG loop and shelf location.

```
Communication Server 1000 Software/Database/  
BOOTROM RMD Install Tool  
  
=====
```

This CS 1000 Call Processor is currently located
in the IPMG configured as:

```
loop 0  
shelf 0
```

Please confirm that the IPMG loop and shelf
information is correct.

Note: If the IPMG has not been configured
yet, the IPMG loop and shelf information can be
left as the current value. To update the loop and
the shelf information later, use OVL117.

Please enter:

```
<CR> -> <y> - Yes, the IPMG loop and shelf  
information is correct.
```

```
<n> - No, the IPMG loop and shelf  
information is incorrect. Go on to Loop/Shelf  
Setting Menu.
```

Enter choice>

- i. Press **y** or **<CR>** to confirm correct IPMG loop and shelf information.

OR

- ii. Press **n** to configure IPMG loop and shelf setting for CP PM card.

- 15 Ensure the RMD containing the installation software is installed in the drive and press **a** or **<CR>**.

```
Communication Server 1000 Software/Database/  
BOOTROM RMD Install Tool  
  
=====
```

Please insert the Removable Media Device into the drive on Core x.

Please enter:

 <CR> -> <a> - RMD is now in drive.
Continue with s/w checking.

 <q> - Quit.

Enter choice> <CR>

The system displays the release of the software found on RMD under the "swload" directory and requests confirmation to continue the installation.

```
Communication Server 1000 Software/Database/  
BOOTROM RMD Install Tool  
  
=====
```

The RMD contains System S/W version xxxx.

Please enter:

 <CR> -> <y> - Yes, this is the correct
version. Continue.

 <n> - No, this is not the correct version.
Try another RMD or a different keycode.

Enter choice> <CR>

- 16 Confirm software installation
- a. If the RMD contains the correct software release, press **y** or **<CR>** and continue to step 17 on [page 115](#).
 - b. If the software release is not correct and you want to replace the RMD, insert the correct RMD in the drive, press **<CR>**, and continue to step 17 on [page 115](#).

- c. If you want to replace the keycode, press **n** and follow the prompts.
- 17** Press **y** or **<CR>** for the Dependency Lists installation and follow the prompts shown in the following example.

Note: If Dependency Lists are not installed on media, the following prompts do not appear. Proceed to step 18 on [page 115](#).

```

Do you want to install Dependency Lists?

Please enter:

<CR> -> <y> - Yes, Do the Dependency Lists
installation

                <n> - No, Continue without
Dependency Lists installation

Enter choice>

The default choice is YES as shown
in the prompt.

If the choice is no, then the
following prompt will appear for the confirmation:

Are you sure?

Please enter:

<CR> -> <n> - No, Go to the Dependency List menu

                <y> - Yes, Go to the next menu

Enter choice>

The default choice is NO which will
return the user to                deplist menu.
    
```

- 18** Enable or disable the Centralized Software Upgrade (CSU) option
- a. Press **y** or **<CR>** to enable the CSU and proceed to step 19 on [page 116](#).
- OR

- b. Press **n** to disable the CSU and proceed to step 20 on [page 117..](#)

```
Enable Automatic Centralized Software Upgrade
(CSU) Feature?

Please enter:

<CR> -> <y> - Yes

<n> - No
```

- 19 Select a CSU upgrade mode:

```
Set Automatic Centralized Software Upgrade Mode
to:

Please enter:

<CR> -> <1> - Sequential

                <2> - Simultaneous

Enter choice>

>Processing the install control file ...

>Installing release 0700x
```

- a. Press **1** or **<CR>** to select sequential upgrade mode. Upgrades to the Media Gateways perform across the LAN in a sequential manner. One Media Gateway is upgraded at a time. No other Media Gateway upgrades are initiated until the current Media Gateway completes its installation.

OR

- b. Press **2** to select simultaneous upgrade mode. Upgrades to the Media Gateways perform simultaneously across the LAN. Up to eight Media Gateways can upgrade at the same time. If there are more than eight Media Gateways, the upgrade to the next Media Gateway begins after the upgrade of one Media Gateway is complete. The following warning is presented to the installer:

```

WARNING:
Call Processing is not guaranteed to operate on
the call server during simultaneous upgrades.
Do you wish to proceed? (y/n)
    
```

Press **y** to proceed with a simultaneous upgrade.

- 20** If the PSDL files menu appears. Select the appropriate choice for your geographic location.

```

*****
PSDL INSTALLATION MENU

The PSDL contains the loadware for all
downloadable cards in the system and loadware for
M3900 series sets.

*****
Select ONE of the SEVEN PSDL files:

1. Global 10 Languages
2. Western Europe 10 Languages
3. Eastern Europe 10 Languages
4. North America 6 Languages
5. Spare Group A
6. Spare Group B
7. Packaged Languages
[Q]uit, <CR> - default

By default option 1 will be selected.
Enter your choice ->x

>Copying new PSDL ...
    
```

- 21 The installation summary screen appears. Verify the parameters and press <CR> when ready.

```
-----
                        INSTALLATION STATUS SUMMARY
-----

+=====+=====+=====+=====+
| Option      | Choice | Status | Comment |
+-----+-----+-----+-----+
| SW: RMD to FMD | yes   |       | install for rel 07.00.xx |
+-----+-----+-----+-----+
| Dependency Lists| yes   |       |           |
+-----+-----+-----+-----+
| AUTO-CSU Feature| SEQ   |       | SEQ-CSU Enabled |
+-----+-----+-----+-----+
| IPMG Software: | yes   |       | install for rel 07.00.xx |
+-----+-----+-----+-----+
| Database       | no    |       |           |
+-----+-----+-----+-----+
| CP-BOOTROM    | yes   |       |           |
+-----+-----+-----+-----+

Please enter:
<CR> -> <y> - Yes, start installation.
       <n> - No, stop installation. Return to the Main Menu.

Enter choice>
>Checking system configuration
```

22 Press <CR> to confirm and continue upgrade.

Note: Once confirmed, the system copies the software from RMD to FMD (the files copied are listed). This file copy takes between 5 and 10 minutes to complete.

```
Please enter:
<CR> -> <y> - Yes, start upgrade.
          <n> - No, stop upgrade. Return to the Main
Menu.

          Enter choice>

>Checking system configuration

You selected to upgrade Software release: XXXX to
release: xxxx. This will erase all old system
files.

This will create all necessary directories and
pre-allocate files on the hard disk.

You may continue with software upgrade or quit
now and leave your software unchanged.

Please enter:

          <CR> -> <a> - Continue with upgrade.
          <q> - Quit.

          Enter choice>
```

- 23** Successful installation confirmation appears, press **<CR>** to continue.

```
Communication Server 1000 Software/Database/  
BOOTROM RMD Install Tool  
  
=====
```

Software release xxxx was installed successfully
on Core x.

All files were copied from RMD to FMD.

Please press <CR> when ready ...

- 24** Press **<CR>** after confirming the Installation summary.

25 The main install menu appears, press **q** to quit.

```

                I N S T A L L   M E N U

The Software Installation Tool will
install or upgrade Succession Enterprise System
Software, Database and the CP-BOOTROM. You will be
prompted throughout the installation and given the
opportunity to quit at any time.

Please enter:

<CR> -> <a> - To install Software, CP-BOOTROM.
        <b> - To install Software, Database,
CP-BOOTROM.
        <c> - To install Database only.
        <d> - To install CP-BOOTROM only.
        <t> - To go to the Tools menu.
        <k> - To install Keycode only.

                For Feature Expansion, use OVL143.
        <p> - To install 3900 set Languages.
        <q> - Quit.

Enter Choice> q
```

26 Confirm quit and reboot. Press <CR> to quit. Press <CR> again to reboot.

```
You selected to quit. Please confirm.

Please enter:

<CR> -> <y> - Yes, quit.

        <n> - No, DON'T quit.

Enter choice> <CR>

You selected to quit the Install Tool.

You may reboot the system or return to the Main
Menu.

-----

DO NOT REBOOT USING RESET BUTTON!!!

-----

Please enter:

<CR> -> <a> - Reboot the system.

        <m> - Return to the Main menu.

Enter Choice> <CR>

>Removing temporary file "/u/disk3521.sys"
>Removing temporary file "/u/disk3621.sys"
>Rebooting system ...
```

The system reloads and initializes.

End of Procedure

To continue a CP PIV or CP PM software upgrade, proceed to Procedure 11 on [page 123](#).

Note: On the Call Server, secure/insecure transfer and shell status will not be changed when restoring the Call Server database.

Verifying the upgraded database

Procedure 11 Verifying the upgraded database

- 1 Log into the Call Server database.
- 2 Print post-upgrade site data in Table 16. Compare a record of the system configuration from the pre-upgrade print out from Table 14 on [page 97](#).

Note: Items marked with an asterisk (*) are required. Other items are recommended for a total system status. Terminal Numbers and Directory Numbers may not be printed depending on size of printed output.

Table 16
Print site data (Part 1 of 4)

Site data	Print command
Terminal blocks for all TNs	LD 20
	REQ PRT
	TYPE TNB
	TN <cr>
	CDEN <cr>
	CUST <cr>
	DATE <cr>
	PAGE <cr>
	DES <cr>
Directory Numbers	LD 20
	REQ PRT
	TYPE DNB
	CUST <cr>

Table 16
Print site data (Part 2 of 4)

Site data	Print command	
Attendant Console data block for all customers	LD 20	LD 20
	REQ	PRT
	TYPE	ATT, 2250
	CUST	<cr>
*Customer data block for all customers	LD 21	LD 21
	REQ	PRT
	TYPE	CDB
	CUST	<cr>
Route data block for all customers	LD 21	
	REQ	PRT
	TYPE	RDB
	CUST	Customer number
	ROUT	<cr>
	ACOD	<cr>
*Configuration Record	LD 22	
	REQ	PRT
	TYPE	CFN
*Software packages	LD 22	
	REQ	PRT
	TYPE	PKG
*Software issue and tape ID	LD 22	
	REQ	ISS
	REQ	TID
* Peripheral software versions	LD 22	
	REQ	PRT
	TYPE	PSWV
	LD 22	

Table 16
Print site data (Part 3 of 4)

Site data	Print command	
Used and unused ISM parameters.	REQ TYPE	PRT SLT
ACD data block for all customers	LD 23 REQ TYPE CUST ACDN	PRT ACD Customer Number ACD DN (or <CR>)
Multi-purpose ISDN Signaling Processor (MISP) card	LD 27 REQ TYPE LOOP APPL PH	PRT MISP loop number (0-158) <cr> <cr>
DTI/PRI data block for all customers	LD 73 REQ TYPE	PRT DDB
Print the configured host information	LD 117	PRT HOST (provides system IP addresses)

Table 16
Print site data (Part 4 of 4)

Site data	Print command
Superloops and XPEs	LD 97 REQ CHG TYPE SUPL SUPL Vxxx V stands for a virtual superloop and xxx is the number of the virtual superloop. xxx = 0-252 in multiples of four for MG 1000E xxx = 96-112 in multiples of four for MG 1000T (See Table 29)
<p>Note: Items marked with asterisks (*) are required printout for conversion. Other items are recommended for a total system status.</p>	

- 3 Print the history file in LD 22 to flag any sysxxx messages.

LD 22 Load program

REQ PRT

TYPE AHST

CUST xx

Press enter until returned to the REQ prompt.

Then **** to Exit program

- 4 Perform a datadump. For CP PIV and CP PM, see “Performing a data dump to backup the customer database:” on [page 134](#).

Reconfiguring I/O parameters and call registers

Procedure 12

Reconfiguring I/O ports and call registers

- 1 For detailed information on call registers, see *Communication Server 1000E Planning and Engineering* (NN43041-220). If changes are required, reconfigure the values in LD 17 below.

Note: If call registers have changed during the upgrade, they do not take effect until the system initializes.

LD 17 Load program

CHG

CFN

PARM YES

500B 1000 Use 1000 as a minimum value

NCR 20000 Use 20000 as a minimum value

Press enter until returned to the REQ prompt.

Then **** to Exit program

2 Print the Configuration Record to confirm the changes made above:

LD 22 Load program

REQ PRT Set the print Option

TYPE CFN Print the configuration

Press enter until returned to the REQ prompt.

Then **** to Exit program

End of Procedure



At this point, all-processing dependent associated applications must be shut down.

Switching call processing to Call Server 1

Note: For network planning best practices refer to *Planning the Network-wide upgrade* (NN43001-406).

Procedure 13
Switching call processing

- 1 Enter LD 135 on Call Server 0 and issue the CUTOVR command. Call processing switches to Call Server 1 and service is interrupted.

LD 135

CUTOVR Transfer call processing from active Call Server
to standby Call Server

**** Exit program

- 2 After Call Server 1 initializes, use the local UCM Administrator account to logon to Call Server 1. Verify that the cutover was successful and that all hardware is operational. Perform acceptance testing as required.



Call Server 1 is now the active CP.

End of Procedure

Upgrade the Voice Gateway Media Card loadware

See “Upgrade the Voice Gateway Media Card loadware” on [page 154](#). Generally, it takes up to 5 minutes to upgrade each Voice Gateway Media Card. A completion message appears for each card when the loadware upgrade is complete.

Upgrading the software on Call Server 0

To upgrade the software on Call Server 0 for CP PIV or CP PM, complete Procedure 10 on [page 106](#) (assume all references to Call Server 1 are now Call Server 0).

Making the system redundant

Procedure 14 Making the system redundant

LD 135	Load program
JOIN	Join the 2 CPUs together to become redundant

Register the Call Server to the security domain

Perform the following procedure to register the Call Server to the security domain. Security domain registration is required if you are upgrading from CS 1000 Release 5.5 or lower, or if the system is not already registered to the UCM security domain.

Procedure 15 Registering the Call Server to the security domain

LD 117	Load program
REGISTER UCMSECURITY SYSTEM FORCE	Register the Call Server to the security domain

You can register and unregister a list of devices with the [**REGISTER / UNREGISTER**] **UCMSECURITY SYSTEM FORCE** command. For more information, see *Security Management* (NN43001-604).

Logoff and login to the Call Server

You must logoff and login to the Call Server using the UCM account that was created when UCM was configured. For details, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Completing the upgrade

Testing the Call Servers

Procedure 16

Testing Call Server 0

At this point in the upgrade, the inactive Call Server is tested from the active Call Server. Upon successful completion of these tests, call processing is switched and the same tests are performed again.

From the active Call Server , perform the following tests on the inactive Call Server:

- 1 Perform a redundancy sanity test:

LD 135

STAT CPU Get status of CPU and memory

TEST CPU Test the CPU

- 2 Check the LCD states

- a. Perform a visual check of the LCDs.
- b. Test and LCDs:

LD 135

DSPL ALL

- c. Check that the LCD display matches the software check.

- 3 Test the System Utility card

LD 135 Load program

STAT SUTL Get the status of the System Utility card

TEST SUTL Test the System Utility card

- 4 Check the system health.
 - LD 135** Load program
 - STAT HEALTH** Check system health

- 5 Test system redundancy and media devices:
 - LD 137** Load program
 - TEST RDUN** Test redundancy

- 6 Clear the display and minor alarms on both Call Servers:
 - LD 135** Load program
 - CDSP** Clear the displays on the cores
 - CMAJ** Clear major alarms
 - CMIN ALL** Clear minor alarms

- 7 Check dial tone.

- 8 Check applications (CallPilot, Symposium, Meridian Mail, etc.)

End of Procedure

Switch call processing

Procedure 17 Switching call processing

- LD 135** Load program
- SCPU** Switch call processing from Call Server
x to Call Server x

End of Procedure

Procedure 18
Testing the Call Server

From the active Call Server , perform these tests on the inactive Call Server:

- 1 Perform a redundancy sanity test:

LD 135 Load program
STAT CPU Get status of CPU and memory
TEST CPU Test the CPU

- 2 Check the LCD states.

a. Perform a visual check of the LCDs.

b. Test LCDs:

LD 135 Load program
DSPL ALL

c. Check that the LCD display matches the software check.

- 3 Test the System Utility card:

LD 135 Load program
STAT SUTL Get the status of the System Utility card
TEST SUTL Test the System Utility card

- 4 Test system redundancy and media devices:

LD 137 Load program
TEST RDUN Test redundancy
******** Exit the program

- 5 Clear the display and minor alarms on both Call Servers:

LD 135 Load program
CDSP Clear the displays on the Call Servers

CMAJ Clear major alarms

CMIN ALL Clear minor alarms

6 Check dial tone.

7 Check applications (CallPilot, Symposium, Meridian Mail, etc.)

End of Procedure

Switching call processing

Procedure 19 Switching call processing

LD 135 Load program

SCPU Switch call processing from the active
Call Server the inactive Call Server

End of Procedure

Performing a customer backup CP PIV/CP PM data dump (upgraded release)

Procedure 20 Performing a data dump to backup the customer database:

1 Log into the system.

2 Insert a CF card into the active Call Server RMD slot to back up the
database.

3 Load the Equipment Data Dump Program (LD 43). At the prompt, enter:

LD 43 Load program.

. EDD

4 When "EDD000" appears on the terminal, enter:

EDD Begin the data dump.



CAUTION

Loss of Data

If the data dump is not successful, do not continue; contact your technical support organization. A data dump problem must be corrected before proceeding.

- 5 When “DATADUMP COMPLETE” and “DATABASE BACKUP COMPLETE” appear on the terminal, enter:

**** Exit program

End of Procedure



The upgrade is now complete.

Upgrading the Signaling Server

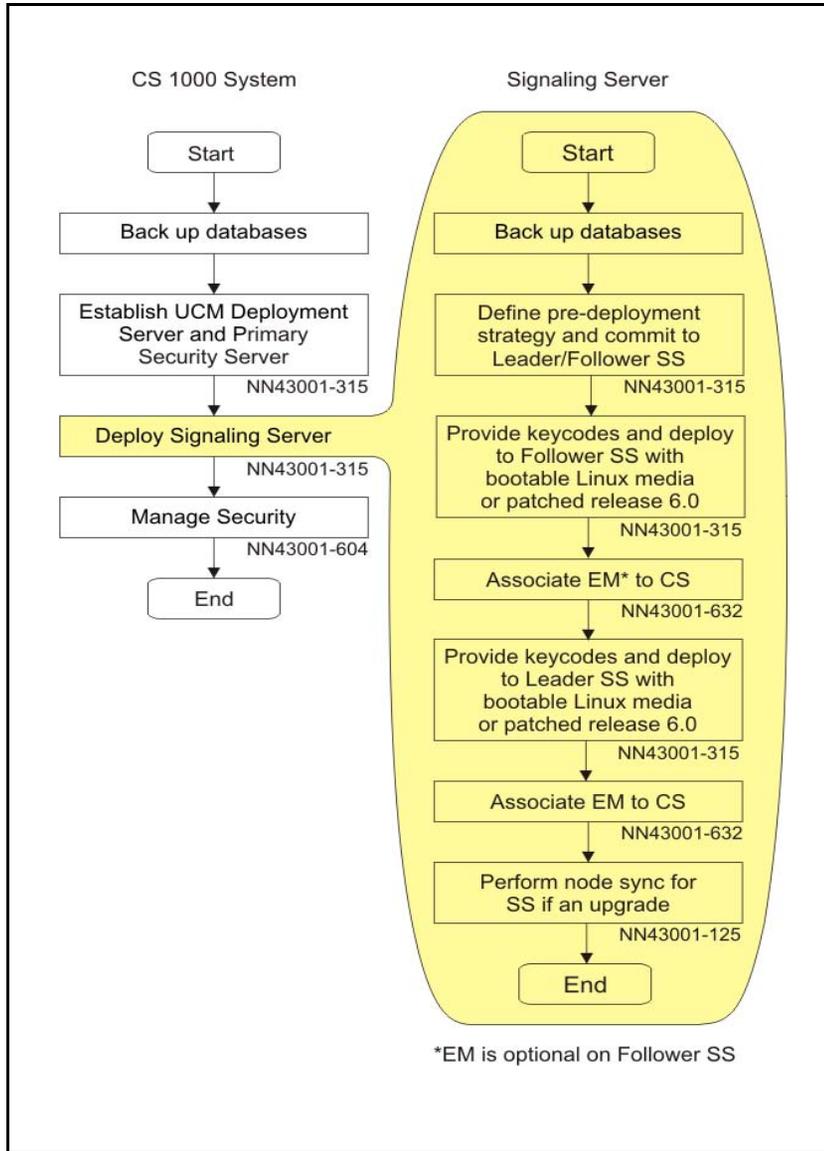
Contents

Taskflow	138
Supported hardware.	140
IP subnet configuration	140
ISP1100 migration.	140
Upgrading and reconfiguring the software	140
NRS	140
Determining the IP Phone firmware version	141
Performing the software upgrade	141
Upgrading and distributing IP Phone firmware	141

Taskflow

Linux Platform Base and Applications Installation and Commissioning (NN43001-315) provides installation and upgrade information for the Linux base and applications. You must follow the proper sequence of events to correctly install or upgrade the Linux base and applications. Use the task flow information below to determine the proper steps for the installation or upgrade of the Linux base and applications.

Figure 12 Signaling Server task flow



Supported hardware

CS 1000 Release 7.0 supports the following Signaling Servers:

- Common Processor Pentium Mobile (CP PM) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
 - IBM X306m server (COTS1)
 - HP DL320 G4 server (COTS1)
 - IBM x3350 server (COTS2)
 - Dell R300 server (COTS2)

IP subnet configuration

If the Signaling Server and Call Server reside in different IP subnets, you must manually add a route from Base Manager in order for Element Manager to communicate and interact with the Call Server. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) for details.

ISP1100 migration

CS 1000 Release 7.0 does not support ISP1100 Signaling Servers. To migrate an ISP1100 Signaling Server to a CS 1000 Release 7.0 platform, see *Signaling Server IP Line Application Fundamentals* (NN43001-125).

Upgrading and reconfiguring the software

NRS

If you do not know whether the Signaling Server being upgraded has an NRS, follow the procedure in *Signaling Server IP Line Application Fundamentals* (NN43001-125) to make this determination.

NRS Servers must be upgraded to CS 1000 Release 7.0 prior to upgrading the first CS 1000 system to CS 1000 Release 7.0. The NRS must operate on the

same software release as the system with the highest software release on the network.

If you have an NRS database on the Signaling Server and wish to back it up prior to the upgrade, you must use the back up tool in NRS Manager. It is recommended that you download the backup file to your local PC after the back up. After the Signaling Server is upgraded, NRS Manager is used to restore the NRS database (from your local PC) and activate it for use by the NRS. For instructions on backing up and restoring an NRS database and IP Phone database, refer to *Signaling Server IP Line Application Fundamentals* (NN43001-125).

Determining the IP Phone firmware version

To determine the version of IP Phone firmware, refer to *Signaling Server IP Line Application Fundamentals* (NN43001-125).

Performing the software upgrade

Signaling Servers run the Linux Base Operating System. This document does not provide information on upgrading Linux Base. For instructions on performing a Signaling Server software upgrade, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) and *Signaling Server IP Line Application Fundamentals* (NN43001-125).

Upgrading and distributing IP Phone firmware

For detailed instructions on how to upgrade and IP Phone firmware to the Signaling Server(s), refer to *Signaling Server IP Line Application Fundamentals* (NN43001-125),

Note: When a firmware upgrade is required for a Branch Office Media Gateway system, install the firmware to the Branch Office TPS before the Main Office TPS. Refer to *Branch Office: Installation and Commissioning* (NN43001-314) for more information.

Upgrading Voice Gateway Media Cards

Contents

This section contains information on the following topics:

Things to know	143
Task summary	146
Verify current loadware versions	146
Determine Voice Gateway Media Card loadware version.....	147
Obtain and upload loadware files	151
Upgrade the Voice Gateway Media Card loadware	154
Upgrade loadware using a Software Delivery card.....	158

Things to know

The Line Terminal Proxy Server (LTPS) portion of the Voice Gateway Media Card application is not supported in CS 1000 Release 7.0. Only the Voice Gateway (VGW) application is supported on all Voice Gateway Media Cards.

During the Signaling Server upgrade, the Install Tool copies Voice Gateway Media Card loadware files to the Signaling Server. Element Manager uses these files to upgrade the Voice Gateway Media Cards to the other components in the IP Telephony nodes.

Before you perform a Voice Gateway Media Card upgrade, verify that the Call Server and Voice Gateway Media Cards are registered to the Security

Domain. Nortel recommends you register all Voice Gateway Media Cards to the same Security Domain as the Call Server.

Secure Shell (SSH) Secure File Transfer Protocol (SFTP) is installed and enabled on CS 1000 Release 7.0 systems by default. This secure protocol replaces regular File Transfer Protocol (FTP) and other insecure data transfer protocols for several CS 1000 applications.

For Voice Gateway Media Cards that cannot be registered to the same Security Domain as the Call Server, you must enable FTP insecure file transfers on the system before performing the upgrade. To support FTP transfers, you must enable FTP on the Call Server, enable FTP on the Voice Gateway Media Cards, and disable SFTP on the Voice Gateway Media Cards. For more information on FTP and SFTP, see *Security Management* (NN43001-604).

For more information about telephone operation during firmware download, see *Signaling Server IP Line Application Fundamentals* (NN43001-125) or *Branch Office: Installation and Commissioning* (NN43001-314).

To upgrade loadware and software, be sure to have the Signaling Server Media from the Upgrades kit on hand.

If an Upgrade kit was not purchased, refer to *Signaling Server IP Line Application Fundamentals* (NN43001-125) for information on how to create a Signaling Server Media.

Alternatively, download the software from the Nortel web site and upload new loadware and firmware from the management workstation to Element Manager. Refer to “Obtain and upload loadware files” on [page 151](#).

Gateway Controller loadware

The Media Gateway Controller (MGC), Media Gateway Extended Peripheral Equipment Controller (MG XPEC), and Common Processor Media Gateway (CP MG) card run the same MGC loadware. A run time check identifies which hardware platform the MGC loadware is running on, controlling the flow of software appropriate for each platform,

If one half of the MG XPEC dual card assembly is not configured, the other configured half functions normally.

The MG XPEC registers to the Call Server as two separate Media Gateway shelves, each with a Media Gateway type of MGX. The MG XPEC card communicates with the Call Server through the ELAN instead of the DS30Y TDM loops used by the previous XPEC card.

The CP MG card registers to the Call Server with a Media Gateway type of MGS. The CP MG card functions as a Server and a Gateway Controller while occupying Slot 0 in a Media Gateway.

Note: The IPMG package must be enabled for the Call Server to accept IP Media Gateway connections.

Table 17 on [page 145](#) provides a list of loadware files used by Gateway Controllers

Table 17 (Part 1 of 2)
Loadware files used by Gateway Controllers

Loadware Name	Description	Notes
MGCCXX##	The CSP load which contains the Nortel code to control the MGX during normal operation.	A run time checks to determine the Gateway Controller platform.
MGCBXX##	This is the boot code.	A run time checks to determine the Gateway Controller platform.
MGCGXX##	The gold image installed at manufacturing.	A run time checks to determine the Gateway Controller platform.
MGCAXX##	This is the application file for special functionality.	A run time checks to determine the Gateway Controller platform.

Table 17 (Part 2 of 2)
Loadware files used by Gateway Controllers

Loadware Name	Description	Notes
MGCFXX##	The FPGA load.	The internal FPGA files are different for the Gateway Controller platforms. The install routine programs the correct file into the FPGA based on platform.
MGCMXX##	Mindspeed load for the Chagall.	
DSP1XX##	Mindspeed load for 96-port DSP DB.	
DSP2XX##	Mindspeed load for 32-port DSP DB.	
DSP3XX##	Mindspeed load for 128-port DSP DB.	

Task summary

To upgrade loadware and software, perform the following tasks:

- 1 Verify the Voice Gateway Media Card loadware version.
- 2 Upgrade the software on all of the Voice Gateway Media Cards.

Verify current loadware versions

Write down the loadware version for each Voice Gateway Media Card. Compare the loadware version with the latest recommended software release on the Nortel web site.

If the Voice Gateway Media Card software are not up-to-date, upgrade the Voice Gateway Media Card with the latest software files.

Determine Voice Gateway Media Card loadware version

To determine the version of loadware on the Voice Gateway Media Card, follow the steps in Procedure 21, Procedure 22, or Procedure 23 on [page 150](#).

Procedure 21

Determining loadware version during boot sequence

- 1 Attach a serial cable from the workstation to the maintenance port of the Voice Gateway Media Card.
- 2 Reset the card.
- 3 Observe the boot sequence and look for a software version message similar to the following example:

```
Software Version: IPL-5.xx  
Management IP: 192.167.100.5  
Host Type: Voice Gateway Media Card  
Firmware Version: MC Firmware Rls 6.7
```

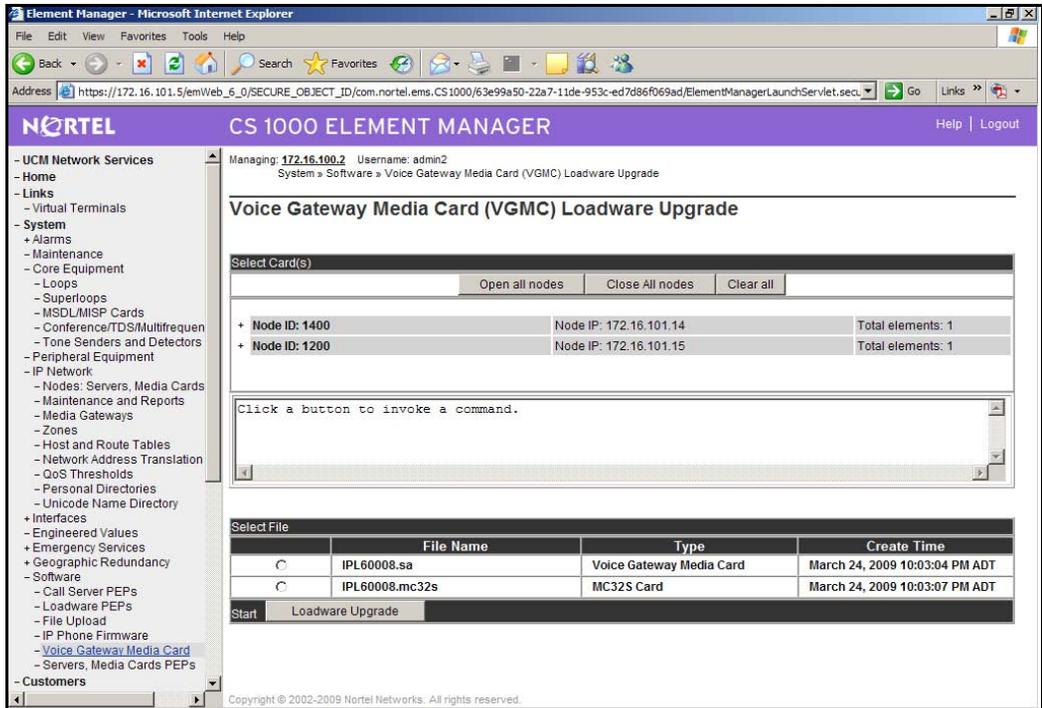
End of Procedure

Procedure 22

Determining the loadware version through Element Manager

- 1 Select **Software** from the System portion of the Element Manager Navigation Tree.
- 2 Click **Voice Gateway Media Card** from the expanded Software menu. The **Voice Gateway Media Card (VGMC) Loadware Upgrade** page appears. See Figure 13 on [page 148](#).

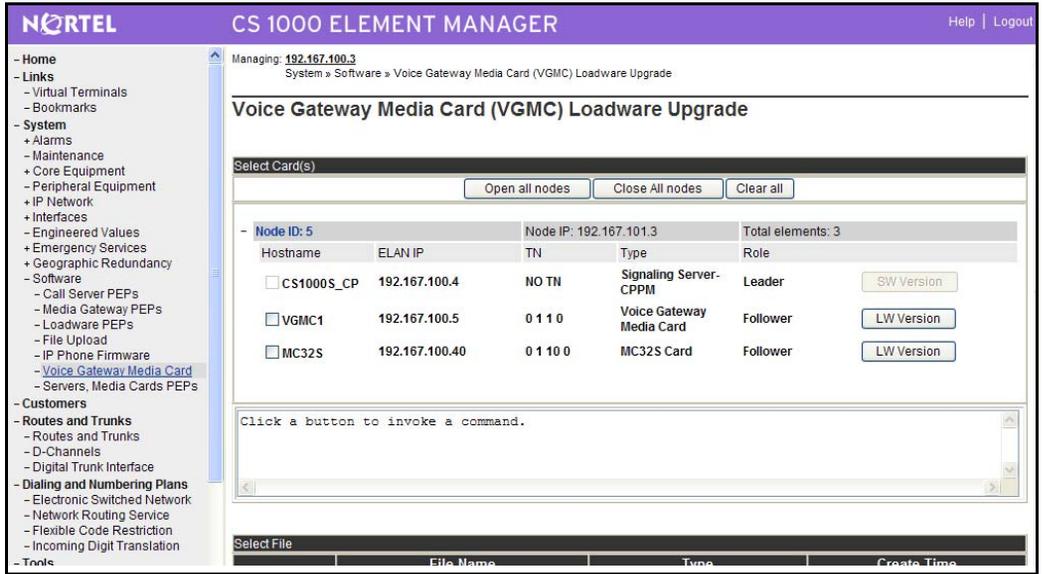
Figure 13
Voice Gateway Media Card (LW) Upgrade window



- 3 Expand a node and select a card in the node.

See Figure 14.

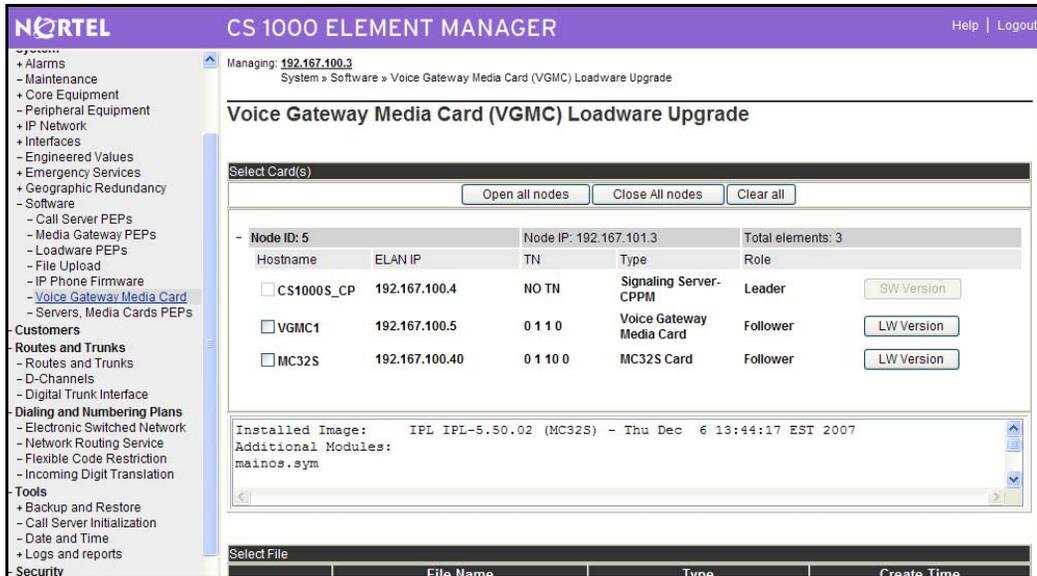
Figure 14
LW Version



- 4 Click the **LW Version** button located to the right of the card information.

The loadware version running on the card is displayed in the pane in the center of the Voice Gateway Media Card (LW) page, as shown in Figure 15 on [page 150](#).

Figure 15
Loadware version displayed



5 Note the loadware version for the card.

End of Procedure

Procedure 23
Determining the loadware version through the CLI

Detailed procedures can be found in *Signaling Server IP Line Application Fundamentals* (NN43001-125).

- 1 Telnet to a Voice Gateway Media Card.
- 2 Log in with a user name and password.
- 3 View the login banner, and look for a software version message similar to the following example:

```

Software Version: IPL-5.xx
Management IP: 192.167.100.5
Host Type: Voice Gateway Media Card
    
```

Firmware Version: MC Firmware Rls 6.7

- 4 Alternatively, view the syslog and look for a software version message.

Note: The Voice Gateway Media Card syslog is also available for viewing from Element Manager.

End of Procedure

Obtain and upload loadware files

This information is provided in the event that the Signaling Server Media is not available. It provides information on how to download the necessary files from the Nortel Software Download web site to a management workstation, and how to upload the Voice Gateway Media Card loadware and IP Phone upgrade firmware from the management workstation to the Signaling Server.

Refer to “Obtaining software” on [page 189](#) for information on how to download the software to a management workstation.

Procedure 24 on [page 152](#) describes how to upload the Voice Gateway Media Card loadware and IP Phone firmware from the management workstation to the Signaling Server. Firmware and loadware upgrade files come with the Signaling Server Media included in the Upgrade kit, or from the Nortel Software Download web site.

If the latest Voice Gateway Media Card loadware and IP Phone firmware files were copied from the CD to the Signaling Server hard drive during the Signaling Server installation, there is no need to follow Procedure 24. If the latest versions of the loadware and firmware are already installed on the Signaling Server, then go to “Upgrading Voice Gateway Media Card loadware” on [page 154](#).

Follow the steps in Procedure 24 to upload the Voice Gateway Media Card loadware and IP Phone firmware from the management workstation to the Signaling Server.

To complete this procedure, use a management PC that is on the same network as the Signaling Server for Element Manager.

Procedure 24

Obtaining and uploading loadware and firmware

- 1 Obtain the latest software installation files for the Voice Gateway Media Card loadware and IP Phone firmware. Download the files from the Nortel Electronic Software Download site to the management PC, as described in “Obtaining software” on [page 189](#).

- 2 Locate the saved files and double-click the *.zip file.

The zipped file opens in a compression utility program and the decompressed files are listed.

For Phase 1 IP Phone 2004, the IP Phone firmware files have the format **'0602BNN.BIN'**

For Phase 1 IP Phone 2002, the IP Phone firmware files have the format **'0603BNN.BIN'**

For Phase 2 IP Phones 2001, 2002 and 2004, the IP Phone firmware files have the format **'0604DNN.BIN'**

where:

06 is the design site location code

02 or 03 is the IP Phone type:

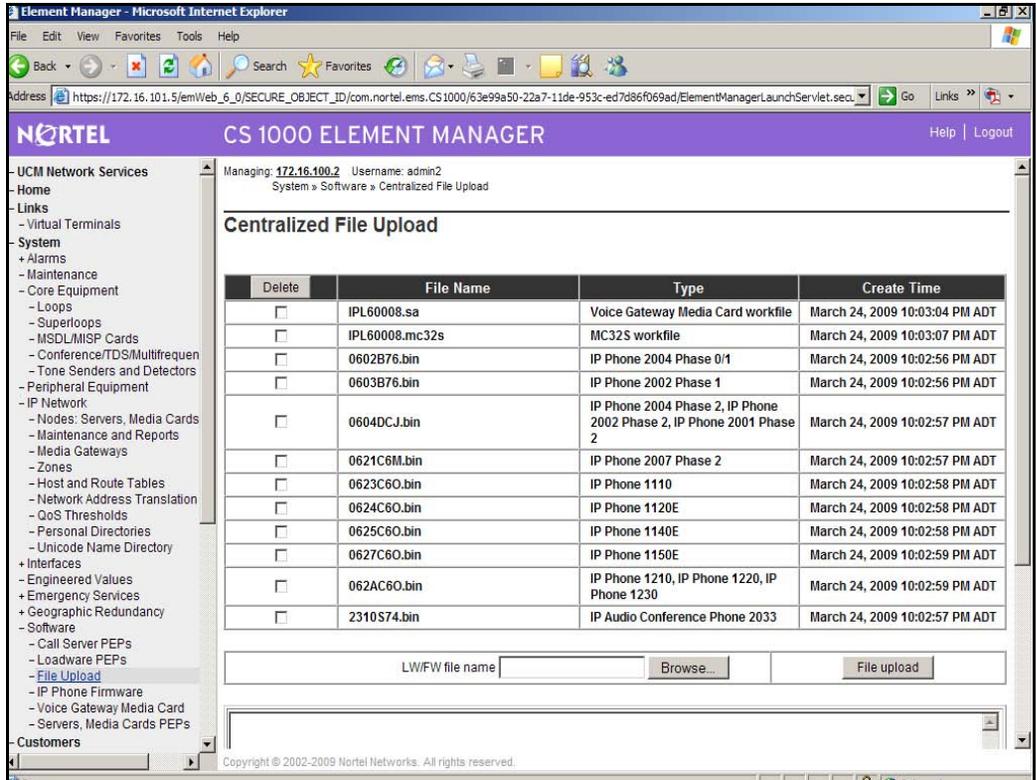
B is the release: {B = 1, C = 2, D = 3 ...}

xx is the firmware version

The Voice Gateway Media Card loadware files have the format **'IPL500xx.mc32s'** and **'IPL600xx.sa'**.

- 3 Log into Element Manager.
- 4 Using **Software> File upload** (see Figure 16 on [page 153](#)), browse to the software files on the workstation and upload them to the Signaling Server.

Figure 16
Upload firmware, software, and loadware



Note 1: After uploading the file to Element Manager, the file remains on this Signaling Server.

Note 2: If there is more than one Signaling Server, the software files uploaded to a specific Signaling Server are not copied to another Signaling Server. It is unnecessary to copy files to other node components, as having a Leader Signaling Server enables central management.

End of Procedure

Upgrade the Voice Gateway Media Card loadware

This section describes how to upgrade Voice Gateway Media Card loadware from 3.x to a later version using Element Manager. The cards obtain their loadware from the Signaling Server.

Follow the steps in Procedure 25 to upgrade Voice Gateway Media Card loadware.

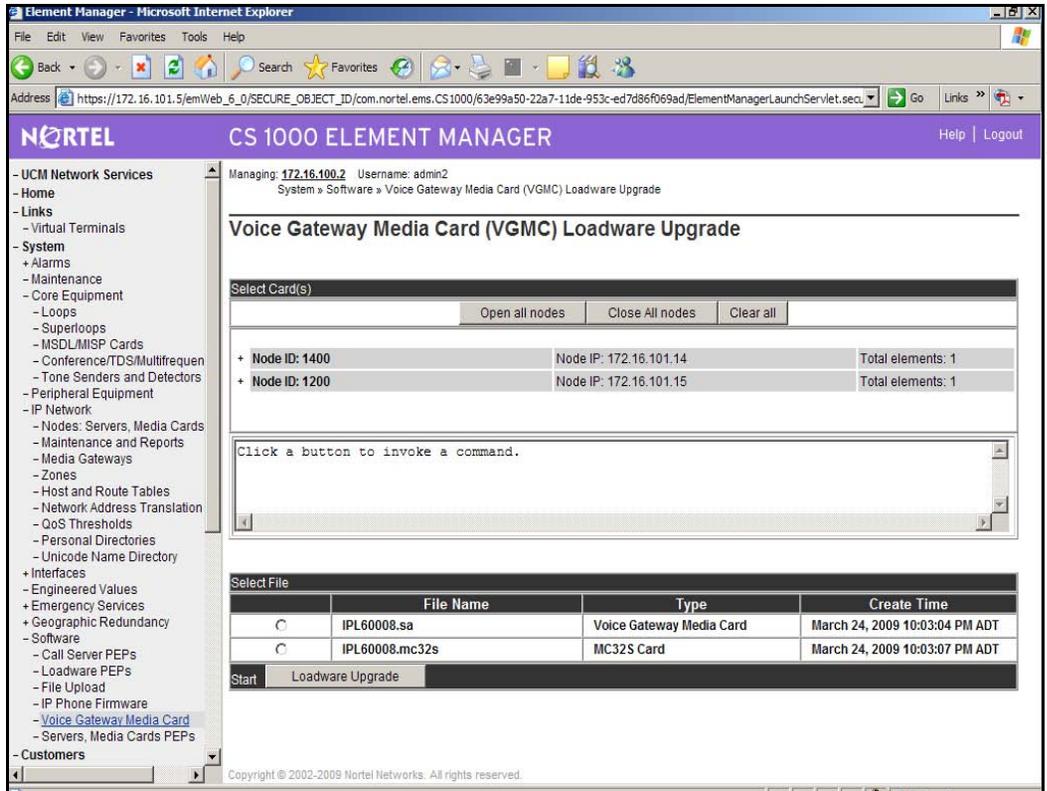
This procedure assumes the Voice Gateway Media Card upgrade loadware has already been uploaded to the Signaling Server. See “Obtain and upload loadware files” on [page 151](#).

Procedure 25

Upgrading Voice Gateway Media Card loadware

- 1 Log into Element Manager.
- 2 For the remote Voice Gateway Media Card upgrade, choose **Software> Voice Gateway Media Card**
- 3 The **Voice Gateway Media Card (VGMC) Loadware Upgrade** window opens. See Figure 17 on [page 155](#).

Figure 17
Voice Gateway Media Card (LW) upgrade



Note: Since components can run different versions of loadware, click the **LW Version** button for a given element to obtain the current loadware version.

- 4 Select the loadware file appropriate to the type of Voice Gateway Media Card that is being upgraded. The filename begins with "IPL".. A sample list of files available is shown in Figure 17.
- 5 Open the node and select the Voice Gateway Media Cards to be upgraded. Select the same type of Voice Gateway Media Card as the loadware file.

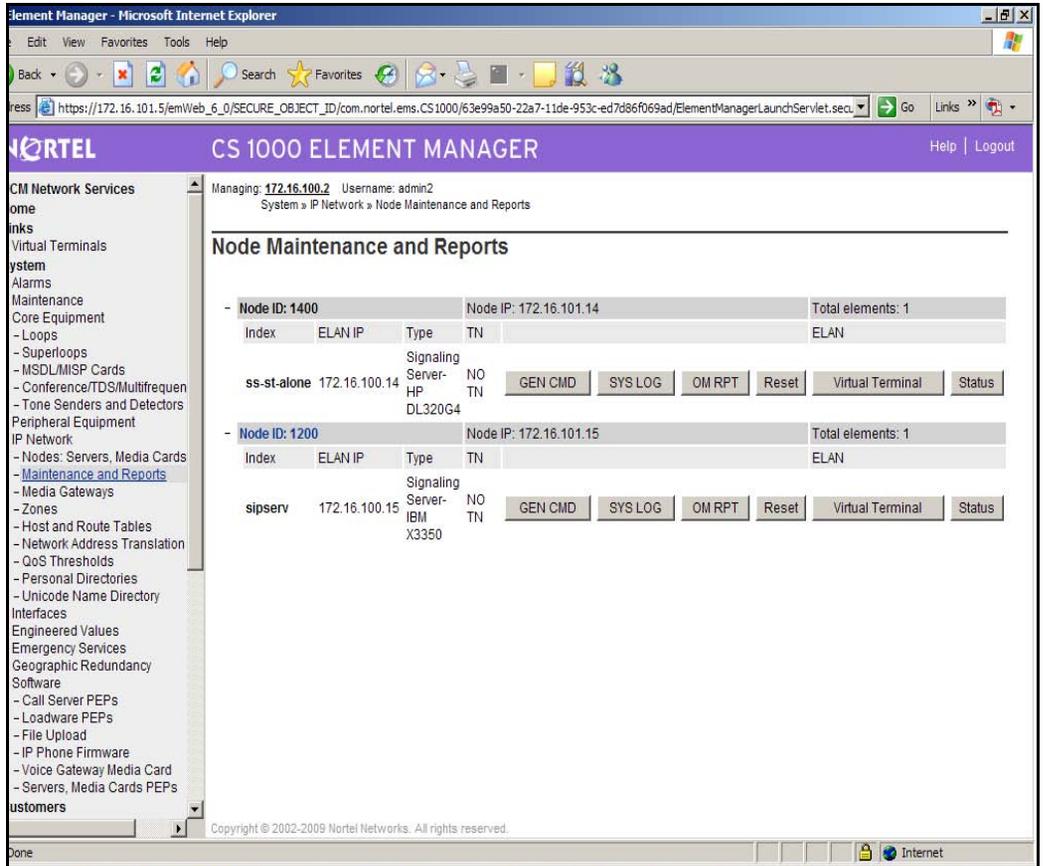
For instance:

- a. If the loadware file has the extension ".sa", only select Media Cards to upgrade.
- b. If the loadware file has the extension ".mc32s", only select MC32S cards to upgrade.

Note: The maximum number of Voice Gateway Media Cards or other components that can be upgraded at a time is four, as all files are simultaneously transferred by FTP.

- 6 Click the **Loadware Upgrade** button on the bottom of the Voice Gateway Media Card (LW) Upgrade window.
- 7 Click **OK** for the confirmation messages.
A Loadware Upgrade Progress page is displayed. When the loadware upgrade is complete, a completion message appears. Generally, it takes up to 5 minutes for each Media Card.
- 8 If the card did not successfully receive the loadware, return to step 2 on [page 154](#). If the upgrade was successful, proceed to step 9.
- 9 Click **IP Network > Maintenance and Reports**. The Node Maintenance and Reports window opens. See Figure 18.
- 10 Click the node to expand it.

Figure 18
IP Telephony information



- Click the **Transfer/Status** button of the Voice Gateway Media Card to be rebooted.

Make sure that the display in the window pane (result box) says:

xx.xxx.xxx.xxx: Disabled.

If this is not displayed, disable the Voice Gateway Media Card. Refer to *IP Line: Description, Installation, and Operation* (NN43100-500). Repeat step 8 again.

- 12 Reboot the card by clicking the **Reset** button for the Voice Gateway Media Card in the Node Maintenance and Reports window (**System > IP Network > Maintenance and Reports**).

See Figure 18 on [page 157](#).

- 13 Look at the faceplate display to determine when the card is finished booting.
- 14 Click the **Status** button for the Voice Gateway Media Card in the IP Telephony Information window and make sure that the message in the window pane (result box) says:

```
xx.xxx.xxx.xxx: Enabled.
```

- 15 Repeat from step 9 on [page 156](#) to step 14 for each Voice Gateway Media Card that received the loadware upgrade.

After the card reboots, transfer IP Telephony node information using Element Manager. Refer to *Signaling Server IP Line Application Fundamentals* (NN43001-125).

End of Procedure

Upgrade loadware using a Software Delivery card

An alternative procedure to using Element Manager for the Voice Gateway Media Card loadware upgrade is using the advanced Command Line Interface (CLI) procedure to upload the files from a Software Delivery Card. For more detailed information, refer to *Signaling Server IP Line Application Fundamentals* (NN43001-125).

Follow the steps in Procedure 26 on [page 159](#) to upgrade the loadware using a Software Delivery Card.

This procedure assumes that the loadware was verified from the CLI as outlined in Procedure 21 on [page 147](#), where a serial cable connects the Voice Gateway Media Card to a workstation.

Procedure 26**Upgrading loadware using a Software Delivery card**

- 1 Download the loadware, as described in “Obtaining software” on [page 189](#). For a first-time Voice Gateway Media Card upgrade after a system upgrade, use the files that are present on the Signaling Server Media.
- 2 Format a Software Delivery card (or delete the old files from the Software Delivery Card) and save the relevant loadware files to the card.

The Voice Gateway Media Card loadware files have the format ‘IPL-----**.sa**’ for the single-slot Media Card.

IMPORTANT!

Do not format the Software Delivery card through Windows or DOS. The file allocation size does not match that of the Voice Gateway Media Card. Use the operating system of the card itself to format the Software Delivery card. Alternatively, simply delete the old files on the Software Delivery Card.

- 3 Reset the card.
- 4 Observe the boot sequence and enter **jkl** when prompted. Be alert as this prompt times out within a few seconds.
- 5 Insert the Software Delivery Card into the Voice Gateway Media Card slot.
- 6 Enter the command:

```
copy "/A:/<filename>" ,"/C:/exec"
```

where <filename> is the name of the file saved to the Software Delivery Card in step 2.
- 7 Remove the Software Delivery Card from the slot of the Voice Gateway Media Card.
- 8 Reset the card.
- 9 Watch the boot messages to confirm the loadware version. Check the release notes to confirm it is the initial version or later.

End of Procedure

Once the Voice Gateway Media Card loadware has been upgraded, verify whether or not the IP Phone firmware also requires an upgrade. Check the loadware release notes to determine which IP Phone firmware versions are compatible with the Voice Gateway Media Cards. If an upgrade is required, refer to “Upgrading and distributing IP Phone firmware” on [page 141](#).

Installing a new keycode

Contents

This section contains information on the following topics:

Introduction	161
Feature operation	162
Feature and License parameter upgrade using a keycode delivered on a CF card	164
Feature and License parameter upgrade using HyperTerminal®	169
Feature and License parameter upgrade entered manually	171
Reverting to the previous keycode with the KRVR command	173

Introduction

Adding new features and/or modifying License limits requires the installation of a new keycode. Keycodes are delivered by a portable media appropriate for the processor type or electronic file transfer. Keycodes can also be manually entered. They are installed using the keycode management commands in LD 143 or the Software Installation Tool.

The following procedures outline the steps to install a new keycode (using the keycode commands in LD 143) that can be activated “instantly” or that requires a Sysload (Cold Restart). More information on the “Instant License” feature can be found in *Features and Services* (NN43001-106).

This section describes how to install a keycode using the commands listed below:

Table 18
Keycode installation

Keycode delivery	Keycode Installation command
CF card for CP PIV, CP PM and CP PM Co-res CS and SS	Use the KNEW RMD command for both Core 0 and Core 1 in LD 143.
USB for Co-res CS and SS	Use KNEW USB
Electronic file on a PC (CP PIV and CP PM only)	Use the KUPL command in LD 143, followed by the KNEW FMD (CP PIV and CP PM) command (see note).
Faxed to the customer site (paper-based keycode for CP PIV, CP PM and CP PM Co-res CS and SS)	Use the KMAN command in LD 143, followed by the KNEW FMD (CP PIV, CP PM and CP PM Co-res CS and SS) command.
<p>Note 1: For a CP PIV and CP PM RMD or USB, the new keycode must be in a file directory called keycode.</p> <p>Note 2: If the keycode is downloaded from the Keycode Distributor Server (KDS), use the KUPL command to install the keycode. Refer to <i>CS 1000M and Meridian 1 Large System Upgrades Overview</i> (NN43021-458) for more information about KDS.</p>	

Feature operation

Feature operation is further broken down into five options:

- Co-res CS and SS keycode validation and pre-configuration using CS 1000 Software Deployment Manager
- Feature and License parameter upgrade using a keycode delivered on a CF card (CP PIV, CP PM and CP PM Co-res CS and SS)
- Upgrade feature and License parameter using HyperTerminal

- Upgrade feature and License parameter entered manually
- Revert to the previous keycode with the KRVR command

Co-resident Call Server and Signaling Server keycode validation and pre-configuration

The CS 1000 Software Deployment Manager provides the following menus and pages specific to Call Server installation and deployment:

- Keycode Validation
- Call Server Database Selection
- Call Server PSDL Language Selection

Prior to deploying the application software to the Co-res CS and SS, the Deployment Manager performs the Call Server keycode validation to ensure that the keycode file used matches the software version and the security device on the target server.

You can use the Deployment Manager to select default, existing, or customer database. The existing database selection does not apply to new installations - only to upgrades. The customer database selection allows the user to upload a Call Server database that has been backed up using the LD 43 EDD command.

Note: After performing the LD 43 EDD command the Co-res CS and SS Call Server database is stored in the `backup/single` folder on the RMD. Click the browse tab and select the backup folder under the **Customer Database** option from Deployment Manager.

The Deployment Manager provides a menu to select the PSDL languages. For a detailed Deployment Manager keycode validation procedure, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Feature and License parameter upgrade using a keycode delivered on a CF card

A directory must be created on the CF card (RMD) named “keycode”. The following rules apply:

- All keycode files must reside in this directory
- The directory can contain up to 20 different keycodes
- The keycode filenames must be unique
- The keycode filenames can contain up to eight characters, and must end with a .kcd extension.

Follow the steps in Procedure 27 on [page 164](#) to perform a feature and License parameter upgrade using a keycode delivered on a CF card.

If HA, leave the system in full redundant mode.

Procedure 27 Performing a feature and License parameter upgrade using a keycode delivered on a CF card.

- 1 Log in on a system terminal and load LD 143.

```
>LD 143  
CCBR000
```

- 2 Insert the new keycode CF card into the CF drive on the active Core.
- 3 Print the pending keycode contents.

KSHO RMD print the contents of the candidate keycode in the CF drive on the active Core. Where:

RMD = Core 0 or 1

- 4 Enter the KDIF command and select keycode comparison options.

Note: Ensure that the new keycode does not lower License limits or reduce features compared with the existing keycode. If it has been determined that the keycode lowers License limits or reduces features, do not continue with the KNEW command. Contact the Nortel order management representative.

. KDIF

Please use: KDIF <param1> <param2> with the following parameters:

NEW	Accepted new keycode
REC	Currently used keycode
OLD	Previously used keycode
RMD	Candidate keycode on removable CF card
FMD	Candidate keycode on fixed CF card

Enter the keycode comparison option. The new keycode option is shown in **bold**.

Note: In the following example, the (REC) currently used keycode will be compared with the new keycode file on the CF card. If choosing from multiple keycode files, ensure you select the correct keycode file. The system limits shown are for example purposes only.

.KDIF REC RMD

Validating Keycode File /p/install/keycode.rec ... OK

The following keycode files are available on the removable media:

Name	Size	Date	Time
-----	-----	-----	-----
<CR> -> <1> - site_A.kcd	1114	Apr-06-2006	10:09
<2> - KEYCODE.KCD	1114	Mar-28-2006	11:11
<p><q> - Quit</p> <p>Enter choice></p>			

Validating Keycode File /cf2/keycode/KEYCODE.KCD ... OK

System parameters	1st keycode	2nd keycode
System Serial Number	: 46379	46379
Software Version	: 3521	3521
System Type	: Option 61C	Option 61C
Call Processor	: CP PIV	CP PIV
Release	: 4	4
Issue	: 50	50
NTI Order Number	:	
NT SDID - 1	:	
NT SDID - 2	:	
Date and Time of Manufacture	:	

Note: (:) indicates that information is not available

License Limits	1st keycode	2nd keycode
Loop Limit	: 32	32
Sys TNs Limit	: 0	200
ACD Agt Limit	: 10	10
ACD DNs Limit	: 10	10
AST Limit	: 10	10

.....

Common packages for both keycodes:

0-2 4-5 7-25 28-29 32-55 58-65

.....

Additional packages in the 2nd keycode:

< **30-31**

.

- 5 Select the new keycode for activation using the KNEW command.

KNEW RMD



CAUTION

A menu appears prompting the user to choose from multiple keycode files. Ensure you select the correct keycode file.

The uploaded keycode is validated against the security device.

If the following system message is displayed:

CCBR020 New Keycode accepted and activated successfully.

Sysload is not needed!

This means that the new keycode is eligible for instant activation and no further user action is required. Go to steps 6 and 7.

If the keycode is not eligible for instant activation, a Sysload is needed to activate the new keycode and the following system message is displayed:

CCBR009 New Keycode accepted. New License limits and feature packages will be activated during the next Sysload (Cold Restart).

Go to step 8.

- 6 Load LD 22 and confirm that the new License parameters have been updated.

```
>LD 22  
REQ SLT
```

....

If License limits are correct, then the keycode installation is complete.

See "Reverting to the previous keycode with the KRVR command" on [page 173](#) if License limits are not increased or problems exist.

- 7 Once it is confirmed that the keycode changes taken effect as expected, perform a data dump in LD 43.

- 8 For keycodes that are not eligible for Instant License, place the system in split mode. This puts a redundant system into single mode.

For CP PIV and CP PM use [Procedure 31](#).

End of Procedure

Feature and License parameter upgrade using HyperTerminal®

Follow the steps in Procedure 28 to perform a feature and License parameter upgrade using HyperTerminal®. Leave the system in full redundant mode.

Procedure 28 Performing a feature and License parameter upgrade

- 1 On a PC, access the system (through a modem) with HyperTerminal®:
Click the Start button | Programs | Accessories | HyperTerminal.
- 2 Double-click the HyperTerminal client to the system.
- 3 Log into the system.
- 4 Load the Keycode Management Program (LD 143).
LD 143 Load program
KUPL Upload keycodes to the hard disk or FMD on the target system
- 5 Click the **Transfer** menu in HyperTerminal and select **Send Text File**.
- 6 From the **Files of type** pull-down menu, select **All Files (*.*)**.
- 7 Locate and select the keycode file on the PC. Use the **Look in** pull-down menu to select the drive on which the keycode is located.
- 8 Click **Open**.

The keycode is displayed after the KUPL prompt.

Example:

```
KUPL 0001PBX 0101
9FPAMSRHNN17KRUQAFFSPREQEVMTIDHRKDJHRKEJR56
```

- 9 Press the Enter key.

The Keycode is checked for CRC errors and is uploaded to the hard disk or Fixed Media Device (FMD).

Enter the following command:

KDIF REC HD Compare the existing keycode with the new keycode on the hard disk

KDIF REC FMD Compare the existing keycode with the new keycode on the FMD

Ensure that the new keycode does not lower License limits or reduce features compared with the existing keycode. If it is determined that the keycode lowers License limits or reduces features, do not continue with the KNEW command. Contact the Nortel order management representative.

- 10 Select the new keycode for activation using the KNEW command.

KNEW (refer to Table 18 on page 162 for correct command syntax)

The uploaded keycode is validated against the security device.

If the following system message is displayed:

CCBR020 New Keycode accepted and activated successfully. Sysload is NOT needed!

This means that the new keycode is eligible for instant activation and no further user action is required. Go to steps 11 and 12.

If the keycode is not eligible for instant activation, a Sysload is needed to activate the new keycode. The following system message is displayed:

CCBR009 New Keycode accepted. New License limits and feature packages will be activated during the next Sysload (Cold Restart).

Go to step 13.

- 11 Load LD 22 and confirm that the new License parameters have been updated.

```
>LD 22
REQ SLT
....
```

If License limits are correct, then the keycode installation is complete.

See “Reverting to the previous keycode with the KRVR command” on [page 173](#) if License limits are not increased or problems exist.

- 12 Once it is confirmed that the keycode changes taken effect as expected, perform a data dump in LD 43.
- 13 For keycodes that are not eligible for Instant License, place the system in split mode. This puts a redundant system into single mode. See [Procedure 31](#).

End of Procedure

Feature and License parameter upgrade entered manually

Before beginning this procedure, obtain a copy of the keycode. The keycode can reside on paper or as an electronic file. To enter the keycode manually, type the keycode in LD 143 as 21 lines, 16 characters per line.

Follow the steps in Procedure 29 on [page 171](#) to perform a feature and License parameter upgrade manually.

Procedure 29

Performing a feature and License parameter upgrade manually

- 1 Log into the system.
- 2 Load the Keycode Management Program (LD 143).

LD 143	Load program
KMAN	Manually enter the keycode to the target system
- 3 Type the keycode file, 21 lines of 16 characters each. Press **Return** to go to the next line.

Note: When entering the keycode, do not enter the header information that proceeds the keycode.
- 4 Type “end” at line 22 to end the process.
- 5 Press **Enter**. The new keycode file is saved on the hard disk or FMD.

Enter the following command:

- | | |
|---------------------|---------------------------------------------------------------------|
| KDIF REC HD | Compare the existing keycode with the new keycode on the hard disk. |
| KDIF REC FMD | Compare the existing keycode with the new keycode on the FMD |

Ensure that the new keycode does not lower License limits or reduce features compared with the existing keycode. If it is determined that the keycode lowers License limits or reduces features, do not continue with the KNEW command. Contact the Nortel order management representative.

- 6 Select the new keycode for activation using the KNEW command.

KNEW (refer to Table 18 on page 162 for correct command syntax)

The uploaded keycode is validated against the security device.

If the following system message is displayed:

CCBR020 New Keycode accepted and activated successfully. Sysload is NOT needed!

This implies that the new keycode is eligible for instant activation and no further user action is required. Go to step 7 and 8.

If the keycode is not eligible for instant activation, a Sysload is needed to activate the new keycode. The following system message is displayed:

CCBR009 New Keycode accepted. New License limits and feature packages will be activated during the next Sysload (Cold Restart).

Go to step 9.

- 7 Load LD 22 and confirm that the new License parameters have been updated.

```
>LD 22
REQ SLT
....
```

If License limits are correct, then the keycode installation is complete.

See “Reverting to the previous keycode with the KRVR command” on [page 173](#) if License limits are not increased or problems exist.

- 8 Once it is confirmed that the keycode changes have taken effect as expected, perform a data dump in LD 43.
- 9 For keycodes that are not eligible for Instant License, place the system in split mode. This puts a redundant system into single mode. See [Procedure 31](#).

End of Procedure

Reverting to the previous keycode with the KRVR command

The terms “old” and “new” keycode, as discussed here, refer to the most recent previous KNEW command. The “old” keycode is the former keycode, prior to the KNEW command. The “new” keycode is the keycode that was activated by the KNEW command. Use KRVR command (as shown in Procedure 30) to revert to the old keycode.

Procedure 30 Revert to old keycode

- 1 Log in to the system.
- 2 Load the Keycode Management Program (LD 143).

LD 143	Load program
KRVR	Replaces the keycode.rec with the keycode.old file.

The old keycode is eligible for instant activation with the KRVR command if the only difference between the old keycode and the new keycode is that some or all of the License parameters in the old keycode are *higher*.

If the old keycode is eligible for instant activation, it is activated without further user action. The following system message is displayed:

**CCBR020 New Keycode accepted and activated successfully.
Sysload is NOT needed!**

If the keycode is not eligible for instant activation, a Sysload is needed to activate the old keycode and the following system message is displayed:

CCBR009 New Keycode accepted. New License limits and feature packages will be activated during the next Sysload (Cold Restart).

Go to step 5.

- 3 Load LD 22 and confirm that the new License parameters have been updated.

```
>LD 22  
REQ SLT  
....
```

If License limits are correct, then the keycode installation is complete.

- 4 Once it is confirmed that the keycode changes taken effect as expected, perform a data dump in LD 43.
- 5 For keycodes that are not eligible for Instant License, place the system in split mode. This puts a redundant system into single mode. See [Procedure 31](#).

End of Procedure

Procedure 31
Parallel reload for CP PIV and CP PM

Place the system in split mode. This puts a redundant (shadowed) system into single (non-shadowed) mode.

- 1 Connect a terminal to J25 of Core 1 to monitor reload. Terminal settings are:
 - 9600 BAUD, 8 bits, no parity and 1 stop bit (8N1)
- 2 Ensure CP 0 is active and CP1 is standby. It might be necessary to switch CPs and split the Cores:

LD 135

STAT CPU

SCPU Switch CPs if necessary

SPLIT Split CPs (CP 1 reloads)

******** Exit program

- 3 Wait until sysload and INI have completed.
- 4 In the inactive core (Core 1), load Overlay 143 and confirm that the new License parameters have been updated.

>LD 143

KSHO REC (show currently used keycode)

....

- 5 Compare license parameters from memory to keycode.rec.

>LD 22

SLT (show current license limits active on system)

....

- 6 Compare package parameters from memory to keycode.rec

```
>LD 22
PRT
PKG (show current software packages active on system)
...
```

- 7 Switch call processing from the active core (Core 0) to the inactive core (Core 1). This command must be issued from active Core 0.



CAUTION — Service Interruption

Service Interruption

Call Processing will be interrupted!

LD 135

CUTOVR

Force Core 1 to become active

Exit program



The previously inactive core (Core 1) with the new keycode now becomes active.

- 8 Return the system to redundant mode, synchronizing the memory and hard drive of the inactive core with the active core. From the active Core (Core 1) enter LD 135:

LD 135

STAT CPU

JOIN

Synchronize CPs with CP 1 as master

Exit program

- 9 Wait until synchronization of memory drives is completed.

- 10 From the active Core (Core 1) enter LD 135 and obtain the health status of the Cores:

LD 135

STAT CPU

STAT HEALTH CP 1 and 0 should have identical health

**** Exit program

- 11 Perform a datadump. The messages "DATADUMP COMPLETE" and "DATABASE BACKUP COMPLETE" will appear once the data dump is complete.

LD 43	
EDD	Begin the data dump
****	Exit program

End of Procedure

Upgrade checklists

Contents

This section contains information on the following topics:

Introduction	177
Site details	178
Upgrade details	178
Pre-upgrade checklists	179
Pre-conversion steps	185
Post-conversion checks	187

Introduction

The following section provides upgrade checklists.

Technical Support

Nortel can provide an Installation and Upgrade Support team to assist with PBX upgrades on a scheduled bases. This service is billable and a purchase order is required. Please refer to current price book for rates.

Note: This service requires that a service request be opened in advance of the upgrade.

Site details

Table 19
Site Details

Customer Name	
Tape ID (LD 22)	
Modem Number (Core)	
Switch Room Telephone	
Baud Rate	
Modem Password	
PBX Password	
System Type	
Software Generic	

Upgrade details

Table 20
Upgrade details

Current Software - Generic	
Target Software - Generic	
Hardware being added	
Feature Upgrade	
License Upgrade	

Pre-upgrade checklists

Software Upgrade

Software audit

Table 21
Software audit

Software Audit		
Perform the software audit prior to the scheduled upgrade.		
Take corrective action if answer is no		
	Yes	No
Software Media Ready		
Keycode Media Ready		
Install Media Ready		
DEP Patch Media Ready Note: Use the MIRCC tool before the upgrade. Meridian ISSP Report and Conflict Checker (MIRCC) Upgrades tool is available on ESPL: https://app91.nortelnetworks.com/espl/		
Review Keycode Data Sheet - (SDID, PKGS, License, TID)		
Review Site Specific Patches - (Non MDCS)		
Read GRB for target Release – (Verify Memory Requirements)		
CP PM VxWorks upgraded to CP PM Cores CS and SS requires 1GByte RMD		
CP PM VxWorks (software only upgrade) requires 512 MByte RMD		

Table 21
Software audit

Cores CS and SS new install – 1GByte RMD		
COTS server install – DVD		
Keycode needed for Subscriber Manager (CS 1000)		
UCM configured		

License Upgrade

Table 22
Keycode audit (Part 1 of 4)

Keycode Audit		
Perform the keycode Audit prior to the scheduled upgrade		
Take corrective action if answer is no		
	Yes	No
Keycode Media Ready		
Keycode Data Sheet Ready		
SDID Matches System		
TID Matches System		
Perform a KDIF in LD 143 to compare keycodes:		

Table 22
Keycode audit (Part 2 of 4)

```

kdif rec fmd
The following keycode files are available on the removable media:
Name                               Size      Date      Time
<CR> -> <1> - CPPM SA PRI 6.0.kcd  1114     Mar-27-2009  13:27

      <2> - CPPM SA SEC 6.0.kcd    1114     Mar-30-2009  13:28

      <q> - Quit

Enter choice> 2

Validating Keycode File /cf2/keycode/CPPM SA SEC 6.0.kcd ... OK
Validating Keycode File /p/install/keycode.rec ... OK

System parameters                1st keycode:      2nd keycode:
System Serial Number              : 46379             46379
Software Version                  : 4021             4021
System Type                       : CS 1000E        CS 1000E
Call Processor                    : CP PM           CP PM
Release                           : 6               5
Issue                             : 0_              50_
NTI Order Number                  : 000000000000    000000000000
NT SDID - 1                       : 00000000        00000000
NT SDID - 2                       : 00000000        00000000
Date and Time of Manufacture      : 30/03/2009     10/12/2007
                                  13:28:28          10:29:17

Note: ( ) indicates that information is not available

Licenses in the                   :1st keycode  2nd keycode:
Loop                              : 1023        1023
Sys TNs                           : 9999 32767

```

Table 22
Keycode audit (Part 3 of 4)

ACD DNs	:	24000	24000
AST	:	9999	32767
LTID	:	100	32760
DCH	:	64	255
AML	:	32	16
MPH DSL	:	100	100
RAN CON	:	9999	32767
RAN RTE	:	9999	512
MUS CON	:	9999	32767
Brand Index	:	2	2
ACD Agents	:	9999	32767
Analogue Telephones	:	0	32767
Attendant Consoles	:	9999	32767
BRI DSL	:	100	10000
CLASS Telephones	:	0	32767
Data Ports	:	9999	32767
Digital Telephones	:	0	32767
IP Users	:	9999	32767
Phantom Ports	:	9999	32767
DECT Users	:	9999	32767
DECT Visitor Users	:	9999	10000
ITG ISDN Trunks	:	9999	32767
Traditional Trunks	:	9999	32767
PCA	:	9999	32767
H.323 Access Ports	:	9999	32767
SIP Access Ports	:	9999	32767
Basic IP Users	:	9999	32767
SIP Converged Desktops	:	10486	32767
SIP CTI TR87	:	4608	32767
Temporary IP Users	:	9999	32767
Mobile Extensions	:	9999	32767
Telephony Services Users	:	9999	32767

Table 22
Keycode audit (Part 4 of 4)

Converged Mobile Users	:	9999	32767
Nortel SIP Lines	:	9999	32767
Third Party SIP Lines	:	9999	32767
 Common packages for both keycodes:			
0-2 4-5 7-14 16-29 32-56 58-65			
67 70-77 79-81 83 86-93 95			
98-103 105 107-111 113-121 125 127			
129 132-133 139-141 145-155 157 159-164			
167 170 172-175 178-181 183-186 191-192			
202-212 214-216 218-219 222-225 227-229 233-235			
240 242-243 245-249 251 253-254 256			
258-259 263 291 296-297 299 301			
305-307 310-313 315-316 321 324 327-334			
336-337 348 350-351 362 364 368			
380-382 384-389 393-394 397-403 406-409 412			
 Additional packages in the 1st keycode:			
<	158 356 396 405 413-418 420		
 Additional packages in the 2nd keycode:			
>	57 104 122-124 126 128 131		
>	134-135 137-138 143-144 169 182 187-189		
>	193 195-196 198 231-232 236 250		
>	255 261-262 283-284 286 288-290 294		
>	308-309 323 325 347 349 366-367		
>	370 404		
.			

Hardware Upgrade

Hardware audit

Table 23
Hardware audit

Hardware Audit		
Perform the Hardware Audit prior to the scheduled upgrade.		
	Yes	No
Verify Shipping List - Complete and Accurate		
Audit Site for new hardware locations		
Pre Run Cables if possible		
Review All switch settings for new cards		
Read all applicable NTP Procedures completely		
CP PM memory upgrade		
SATA controller upgrade kit for IBM COTS servers		

Pre-conversion steps

Table 24
Pre-conversion steps (Part 1 of 2)

Pre Conversion Steps
A capture file should be made of the following information using a PC or Printer.
Perform an overall system check:
LD 135 SCPU (ensure that the system is redundant)
LD 137 STAT/TEST CMDU
LD 48 STAT AML
LD 32 STAT

Table 24
Pre-conversion steps (Part 2 of 2)

LD 60 STAT
LD 30 LDIS (Verify what is disabled if any)
Get Software Information from LD 22
ISSP - Patches in service - Future Reference if required
TID/SLT - License Parameters - To compare with converted database
LD 21 - PRT CFN
LD 97 - PRT SUPL/XPEC
Run a Template Audit
LD 1 - Auto Run
Perform a Datadump
Backup at least two copies of the current database, retain the copies.
Print History File or System Event Log
Ld 22 - Print AHST - Capture Systems Events to compare with new software if required
Ld 117 - PRT SEL 500 - Same as above
Derive FQDN's for TLAN IP devices
Identify all IP addresses for all devices
Radius Authentication – IP Address Secret Key recorded
PD database backed up
Derive the list of users and their roles (which could be important in executing day to day activities)
Disable IPSEC

Post-conversion checks

Table 25
Post-conversion checks

Post Conversion Checks
Perform these checks after a successful INI.
Test for dial tone
Ensure that all AUX applications are working
LD 30 LDIS (Verify that output is the same prior to upgrade)
Test out basic, typical call scenarios that worked prior to the upgrade. Verify test calls over any SIP or PRI trunks. Verify IP to TDM calls if Media Cards are present.
Verify successful log in to various devices, UCM, Signaling Server, and Call Server using appropriate credentials.
Perform a physical check of the hardware. Ensure LED's are green. Verify the LED status of the PRI, activity lights on MGC Ethernet connections. MGC faceplate must display valid data.
Check IPSEC and Token Generation by logging into UCM. Click the IPSEC tab to verify the synchronization of all elements. Click the Secure FTP Token tab to verify Token synchronization.

Appendix A: Obtaining software

Downloading software from the Nortel website

It is not necessary to acquire software media from Nortel to begin a system upgrade. The software is available from the Nortel Software Download website. Keycodes are required in order for the software installation to work.

Check the Nortel Software Download web site for the latest software and firmware releases.

Note: See the Ordering Rules and Price Book from a Nortel supplier for details on items and packages.

Follow the steps in Procedure 32 to download software from the Nortel Software Download web site

Procedure 32

Downloading software from the Nortel website

- 1 Connect to the following URL using any PC with Internet access:
<http://www.nortel.com>
- 2 If not already logged into a My Nortel account, enter a User ID and Password on the **Sign In** page and then click **Sign In**.
- 3 Under the **Support and Training** menu, select **Software Downloads > Product Family >Voice, Multimedia, and Unified Communications**.
- 4 Under the heading **IP-Enabled & Pure IP Networks**, select **IP Line and Voice Gateway Media Cards (VGMC)**.

5 Click **Releases**.

————— **End of Procedure** —————

Technical Assistance service

Contents

This section contains information on the following topics:

Nortel Technical Assistance Centers	191
Services available	194
Requesting assistance	197

Nortel Technical Assistance Centers

To help customers obtain maximum benefit, reliability, and satisfaction from their CS 1000E systems, Nortel provides technical assistance in resolving system problems. Table 26 on [page 192](#) lists the centers that provide this service.

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

If a Nortel service program was purchased, contact one of the following Nortel Technical Solutions Centers.

Table 26
Customer Technical Services (Part 1 of 2)

Location	Contact
Nortel Global Networks Technical Support (GNTS) PO Box 833858 2370 Performance Drive Richardson, TX 75083 USA	North America Telephone: 1 800 4NORTEL
Nortel Corp. P.O. Box 4000 250 Sydney Street Belleville, Ontario K8N 5B7 Canada	North America Telephone: 1 800 4NORTEL
Nortel Service Center - EMEA	EMEA Telephone: 00 800 8008 9009 or +44 (0)870 907 9009 E-mail: emeahelp@nortel.com
Nortel 1500 Concord Terrace Sunrise, Florida 33323 USA	Brazil Telephone: 5519 3705 7600 E-mail: entcts@nortel.com English Caribbean Telephone: 1 800 4NORTEL Spanish Caribbean Telephone: 1 954 858 7777 Latin America Telephone: 5255 5480 2170

Table 26
Customer Technical Services (Part 2 of 2)

Location	Contact
Network Technical Support (NTS)	<p>Asia Pacific Telephone: +61 28 870 8800</p> <p>Australia Telephone: 1800NORTEL (1800 667835) or +61 2 8870 8800 E-mail: asia_support@nortel.com</p> <p>People's Republic of China Telephone: 800 810 5000 E-mail: chinatsc@nortel.com</p> <p>Japan Telephone: 010 6510 7770 E-mail: supportj@nortel.com</p> <p>Hong Kong Telephone: 800 96 4199 E-mail: chinatsc@nortel.com</p> <p>Taiwan Telephone: 0800 810 500 E-mail: chinatsc@nortel.com</p> <p>Indonesia Telephone: 0018 036 1004</p> <p>Malaysia Telephone: 1 800 805 380</p> <p>New Zealand Telephone: 0 800 449 716</p> <p>Philippines Telephone: 1 800 1611 0063 or 632 917 4420</p> <p>Singapore Telephone: 800 616 2004</p> <p>South Korea Telephone: 0079 8611 2001</p> <p>Thailand: Telephone: 001 800 611 3007</p>

Services available

Services available through the Technical Assistance Centers include:

- diagnosing and resolving software problems not covered by support documentation
- diagnosing and resolving hardware problems not covered by support documentation
- assisting in diagnosing and resolving problems caused by local conditions

There are several classes of service available. Emergency requests (Class E1 and E2) receive an immediate response. Service for emergency requests is continuous until normal system operation is restored. Non-emergency requests (Class S1, S2, and NS) are serviced during normal working hours. Table 27 on [page 195](#) and Table 28 on [page 196](#) describe the service classifications.

Table 27
Technical service emergency classifications

Class	Degree of failure	Symptoms
E1	Major failure causing system degradation or outage	<p>System out-of-service with complete loss of call-processing capability.</p> <p>Loss of total attendant console capability.</p> <p>Loss of incoming or outgoing call capability.</p> <p>Loss of auxiliary Call Detail Reporting (CDR) in resale application.</p> <p>Call processing degraded for reasons such as trunk group out-of-service:</p> <ul style="list-style-type: none"> • 10% or more lines out-of-service • frequent initializations (seven per day or more) • inability to recover from initialization or SYSLOAD • consistently slow dial tone (eight seconds or more delay)
E2	Major failure causing potential system degradation or outage	<p>Standby CPU out-of-service.</p> <p>Frequent initializations (one per day or more).</p> <p>Disk drive failure.</p> <p>Two sets of disks inoperative.</p>

Table 28
Technical services non-emergency classifications

Class	Degree of failure	Symptoms
S1	Failure that affects service	<p>Software or hardware trouble directly and continuously affecting user's service or customer's ability to collect revenue.</p> <p>Problem that will seriously affect service at in-service or cut-over date.</p>
S2	Intermittent failure that affects service	<p>Software or hardware faults that only intermittently affect service.</p> <p>System-related documentation errors that directly result in or lead to impaired service.</p>
NS	Failure that does not affect service	<p>Documentation errors.</p> <p>Software inconsistencies that do not affect service.</p> <p>Hardware diagnostic failures (not defined above) that cannot be corrected by resident skills.</p> <p>Test equipment failures for which a backup or manual alternative can be used.</p> <p>Any questions concerning products.</p>

Except as excluded by the provisions of warranty or other agreements with Nortel, a fee for technical assistance may be charged, at rates established by Nortel. Information on rates and conditions for services are available through Nortel sales representatives.

Requesting assistance

Collect the information listed in Table 29 before you call for service.

Table 29
Checklist for service requests

Name of person requesting service	_____
Company represented	_____
Telephone number	_____
System number/identification	_____
Installed software generic and issue (located on data disk)	_____
Modem telephone number and password (if applicable)	_____
Seriousness of request (see Tables 27 and 28)	_____
Description of assistance required	_____

Nortel Communication Server 1000
Communication Server
1000E
Software Upgrades

Copyright © 2004-2010 Nortel Networks. All rights reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing. NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo and the Globemark are trademarks of Nortel Networks. All other trademarks are the property of their respective owners.

Publication number: NN43041-458
Document release: 04.03
Date: July 2010

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

