Nortel Communication Server 1000

Planning the Network-wide Upgrade

Release: 7.0
Document Revision: 04.01

www.nortel.com

NN43001-406

Nortel Communication Server 1000
Release: 7.0
Publication: NN43001-406
Document release date: 4 June 2010

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.

Contents

New in this release

The following sections details what’s new in *Planning the Network-wide Upgrade* (NN43001-406) for Nortel Communication Server (CS) 1000 Release 7.0.

Navigation

- “Feature changes” (page 5)
- “Other changes” (page 8)

Feature changes

Following are the new features introduced in CS 1000 Release 7.0:

- **High Scalability**

  -- A High Scalability (HS) system contains multiple CS 1000 High Availability (HA) systems that are centrally managed using Element Manager HS.
- **Patching Management enhancements** -- Central Patching Manager now supports binary patches and deplists for VxWorks elements, such as Call Servers and Media Cards, as well as MGC and PSDL loadware patching.
- **SNMP Profile distribution** -- SNMP Profile Manager displays all elements registered to the UCM Security domain in a tree view. You can select up to a maximum of 500 individual elements or groups of elements for system-wide profile distribution.
- **UCM security domain** --A Unified Communication Management (UCM) security domain is defined by the UCM primary security server. The UCM security domain comprises the UCM primary security server, the UCM backup security server, and associated member servers that contain UCM Common Services and management applications. The primary security service or backup security service is not installed on a member server.

For more information about UCM security domain, see "Security domain" (page 30)

- **Central authentication** --The UCM Common Services provides a centralized GUI-based interface for individual account administration for the Communication Server 1000 network. This authentication feature implements a RADIUS client that authenticates with the external UCM security server for all VxWorks software and Linux platforms that are supported by the current Communication Server 1000 software release. It contains all system elements registered to the UCM security domain, including:

  — Call Server

  — Signaling Server

  — MGC

  — VGMC

- **UCM tools** --The central UCM primary security server uses the log viewer tool to view Security and Operation, Administration, and Maintenance (OAM)-related audit logs.

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

- **ISSS enhancements** --The Intra System Signaling Security (ISSS) synchronization feature has an improved user interface and improved security. ISSS is included as part of the UCM installation and is user configurable on the Primary Security server.

  Intra-System Signaling Security (ISSS) supports two levels: Optimal and Full. Both these levels are more restrictive than in past releases, in that protocols are enforced rather than permissive.

  > **ATTENTION**
  > ISSS Full is required to protect AML.

  For more information about ISSS security levels, see "Intra-System Signaling Security or IPsec" (page 31).

  For more information, see *Security Management Fundamentals* (NN43001-604).

- **SNMP profiles** --A network level SNMP configuration capability is introduced using the SNMP Profile Manager. Users may wish to switch to using this network level configuration. The system level configuration of SNMP using Element Manager or Call Server CLI continues to be supported.

For more information about the SNMP profiles see *Communication Server 1000 Fault Management — SNMP* (NN43001-719).

- **Secure transport enhancements** --The SSH File Transfer Protocol (SFTP) is introduced in this release as a security feature. The exchange of files internal to the system and externally over the IP network can be carried out with the SFTP instead of conventional FTP.
- **Patch management enhancements** --
  - — handles the patch conflict issues under patch obsolescence
  - — increases the capability of special instructions
  - — introduces patch dependency
- **Element Manager** --For CS 1000 Release 7.0, one instance of Element Manager manages one CS 1000 Release 7.0 system, and normally runs on a Linux base element local to that system. For more information, see *Element Manager System Reference - Administration* (NN43001-632).
- **NTP enhancements --**For Network Time Protocol (NTP), a new model has been introduced for CS 1000 systems for CS 1000 Release 6.0. This involves having internal primary and secondary NTP servers running on Linux system elements. When upgrading to CS 1000 Release 6.0, it is essential to use Element Manager to re-configure NTP settings or other time synchronization schemes. Linux base elements can also directly synchronize with external NTP clock sources. You can configure this using Base Manager. For more information, see “Network Time Protocol configuration” (page 34).
- **UNIStim security with DTLS** --UNIStim security with DTLS provides:
  - — secure transport services for applications based on datagram protocols, for example, UDP
  - — integrated solution that is both more scalable and more manageable

  DTLS is controlled by a tri-state setting DTLS off, DTLS when possible and DTLS only. The default setting is DTLS when possible.

  To configure or upgrade the network, the following three levels of DTLS security are introduced:

  - — Basic Security
  - — Advanced Security
  - — Complete Security

For more information about these security levels see “Datagram Transport Layer Security” (page 33).

Two sub-prompts DTLS ClientAuthentication and DTLS Renegotiation are displayed when DTLS Only or DTLS On is selected for DTLS policy in order to enable DTLS functionality.

Three new commands are introduced in **General Commands** page for “Iset” group: `isetSecGet`, `isetSecShow`, `isetSecUpdate`. `tpsShow` Command output is enhanced to show the DTLS results.

- Following hardware platforms are not supported in this release:
  - CP PII
  - SSC
  - ITG Pentium
  - ISP 1100
  - ITG IP Trunk

Other changes

Revision history

June 2010	Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.0.
July 2009	Standard 03.17. This document is up issued to reflect changes made to section Planning considerations for the network-wide upgrade.
June 2009	Standard 03.16. This document is issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.15. This document is issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.14. This document is issued to support Communication Server 1000 Release 6.0.
December 2007	Standard 02.02. This document is issued to support Communication Server 1000 Release 5.5.
May 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0. No new content has been added for Communication Server 1000 Release 5.0. All references to Communication Server 1000 Release 4.5 are applicable to Communication Server 1000 Release 5.0.

Introduction

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

Subject

This document includes the following information:

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

Note on legacy products and releases

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

www.nortel.com

Applicable systems

Server cards

- Nortel Common Processor Pentium Mobile (CP PM)
- Common Processor Dual Core (CP DC)
- Common Processor Media Gateway (CP MG) 32
- Common Processor Media Gateway (CP MG) 128

The Server cards can host a Co-resident Call Server and Signaling Server configuration in CS 1000 Release 7.0. For more information, see *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

COTS Servers

- IBM x306m (COTS1)
- HP DL320-G4 (COTS1)
- IBM x3350 (COTS2)
- DELL R300 (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 Nortel CP PM and CP DC platforms are circuit cards hosted in Media Gateway slots in CS 1000E systems or in slots of Universal Equipment Modules (UEM) in CS 1000M SG and CS 1000M MG systems. The CP MG platform is a circuit card and is hosted in slot 0 of a Media Gateway in CS 1000E systems.

The other platforms are commercial off-the-shelf (COTS) servers. For more information about the platforms, and instructions to install, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

All hardware platforms have an ELAN and a TLAN network interface. The IP Line applications communicate with the system Call Processor through the system ELAN subnet.

ATTENTION
When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 6.0 software and configured to include a Signaling Server, they become CS 1000M systems. Table 1 "Meridian 1 systems to CS 1000 Release 7.0 systems" (page 10) lists each Meridian 1 system that supports an upgrade path to a CS 1000 Release 7.0 system.

Table 1
Meridian 1 systems to CS 1000 Release 7.0 systems

This Meridian 1 system...	Maps to this CS 1000 Release 7.0 system
Meridian 1 PBX 11C Chassis	CS 1000E
Meridian 1 PBX 11C Cabinet	CS 1000E
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81C	CS 1000M Multi Group

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

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

Intended audience

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

Terminology

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

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

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

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

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

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

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

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

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

Table 2
Hardware platform supported roles

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

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

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

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *SIP Line Fundamentals* (NN43001-508)

- *Security Management Fundamentals* (NN43001-604)
- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Product Compatibility Reference* (NN43001-256)
- *Dial Plans Reference* (NN43001-283)
- *IP Peer Networking Installation and Commissioning* (NN43001-313)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *System Management Reference* (NN43001-600)
- *Emergency Services Access Fundamentals* (NN43001-613)
- *IP Trunk Fundamentals* (NN43001-563)
- *Telephones and Consoles Fundamentals* (NN43001-567)
- *ISDN Primary Rate Interface Fundamentals* (NN43001-569)
- *Basic Network Feature Fundamentals* (NN43001-579)
- *Communication Server 1000M and Meridian 1 Small System Software-only Upgrade* (NN43011-459)
- *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)
- *Communication Server 1000S: Upgrade Procedures* (NN43031-458)
- *Communication Server 1000E Software Upgrades* (NN43041-458)

Online

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

www.nortel.com

CD-ROM

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

Software requirements

This chapter describes the relative software versions required in the Main office and Branch Office locations. The actual software packaging requirements are given in "Main office requirements" (page 17) and "Branch Office requirements" (page 18). It contains information on the following topics:

Main office and Branch Office running the same release

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

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

Main office and Branch Office running different releases

It is recommended that the software release on the Branch Office always match the software release on the main office. However, the main office Call Server and the Branch Office can have different software releases, as long as the main office runs at the higher release. With the main office running Communication Server 1000 Release 6.0 software the Branch Office must run Communication Server 1000 Release 6.0, Release 5.5, or Release 5.0.

Indefinite operation with a mixed-software configuration of Communication Server 1000 Release 4.5 and Communication Server 1000 Release 5.0 Branch Offices with a Communication Server 1000 Release 5.5 main office is supported.

Consider this mixed software policy when planning your system upgrade. Branch Offices must be at Communication Server 1000 Release 4.5 or later prior to upgrading the main office to Communication Server 1000 Release 5.5 to ensure a supported configuration during the upgrade period.

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

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

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

Features in mixed-software configuration

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

If the Branch Office is running a lower release of software than the main office, features involving interaction between the main office and the Branch Office does not function for the Branch Office IP Phone users. For example, if the main office is on Communication Server 1000 Release 7.0 and the Branch Office is on Communication Server 1000 Release 5.0 or 5.5, features introduced in CS 1000 Release 7.0 will not operate for the Branch Office IP Phone users since these features are not supported on earlier releases. In this case, the Branch Office would need to be upgraded to Communication Server 1000 Release 6.0 to support these features.

Adding a Branch Office to an existing network

For customers wanting to add a Branch Office to their existing network, customers are still permitted to order a Branch Office running Communication Server 1000 Release 5.0 if their main office is running Communication Server 1000 Release 5.0. They are also permitted to order a Branch Office running Communication Server 1000 Release 4.5 and 4.0 if the main office is running Communication Server 1000 release 4.5 and 4.0.

ATTENTION
Both the Call Server and Signaling Server in an office must run the same release of software. The main office must always run CS 1000 Release 4.5 on the Call Server and the Signaling Server.

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

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

Main office requirements

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

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

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

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

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

- Network Attendant Service (NAS) package 159 -- This package is required for analog (500/2500-type) telephones in the Branch Office to access attendant services when the attendant is configured on the main office.
- Network Message Services (NMS) package 175 -- This package is required for analog (500/2500-type) telephones in the Branch Office to

share the voicemail system in the main office. For any configurations using centralized Call Pilot on the main office with one or more Branch Offices in separate time zones, the NMS package is required at the main office for the branch IP Phones.

Optional features

- Network Alternate Route Selection (NARS) package 58. For more information, see *Basic Network Feature Fundamentals* (NN43001-579).
- Overlap Signaling (OVLP) package 184. This package is optional; it is required for overlap signaling. It is packaged with H.323 Virtual Trunk (H323_VTRK) package 399 (Release 4.0 and Release 4.5).
- Emergency Services Access (ESA) package 329. This package is optional and is required to receive 911/ESA features. For more information, see *Emergency Services Access Fundamentals* (NN43001-613).
- Virtual Office (VIRTUAL_OFFICE) package 382 and M3900 Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387. These packages are optional; they are required only for Virtual Office functionality.
- Network Signaling (NSIG) package 37. This package is optional for SRG IP Phones to access set-based Network Class of Service (NCOS) features.
- Adaptive Network Bandwidth Management package 407.
- Alternate Routing for Network Bandwidth Management.
- SIP Gateway and Converged Desktop (SIP) package 406. This package is optional; it is required to support SIP functionality.

Branch Office requirements

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

- Command Status Link (CSL) package 77
- Integrated Services Digital Network (ISDN) package 145
- Flexible Numbering Plan (FNP) software package 160. For more information, see *Dialing Plans Reference* (NN43001-283).
- Overlap Signaling (OVLP) package 184. This package is required only if overlap signaling is to be implemented in the Branch Office.

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

- Enhanced ACD Routing (EAR) package 214
- Enhanced Call Trace (ECT) package 215
- Emergency Services Access (ESA) package 329
- Virtual Office (VIRTUAL_OFFICE) package 382 and M3900 Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387. These packages are optional; they are required only for Virtual Office functionality.
- BMG package 390
- IP Peer H.323 Trunk (H323_VTRK) package 399. This package is optional; it is required for H.323 functionality. The packaging for package 399 also includes package 184.

ATTENTION
These packages are automatically enabled in the Branch Office software.

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

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

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

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

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

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

Main office and Branch Office

This section describes the existing rules for software release compatibility between main office and Branch Offices. It is possible for a main office Call Server and the Branch Office MG 1000B to temporarily have different software releases, if the main office is running the newest release (CS 1000 Release 5.5 software). For example, a Branch Office may run a different software release than that (2.0 / 3.0 / 4.0) associated with a CS 1000 Release 4.0 main office Call Server.

By allowing this mixed software operation, customers do not have to upgrade their entire network of Branch Offices in order to add a single additional Branch Office running CS 1000 Release 5.5 software. This permits the network upgrade to be scheduled over a longer period. The main office Call Server must be running the highest available release of software. Issues within a release are considered equivalent.

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

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

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

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

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

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

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

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

Main office to main office - peer interworking

Table Table 3 "Peer interworking - main office to main office " (page 21) shows the peer interworking between any combinations of the software releases 6.0, 5.5, 5.0, 4.5, 4.0, and 3.0.

Table 3
Peer interworking - main office to main office

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

Main office to Branch Office - peer interworking

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

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

Table Table 4 "Branch - one release back" (page 21) shows supported Mixed Main/Branch combinations for Branch that is one release back:

Table 4
Branch - one release back

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

Table Table 5 "Branch - two releases back" (page 22) shows supported Mixed Main or Branch combinations for Branch that is two releases back:

Table 5
Branch - two releases back

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

Geographic redundancy

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

> **ATTENTION**
> Only GR 1+1 is supported. GR N+1 is not supported.

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

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

Geographic redundancy operation

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

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

- — Client tries registration with GRS SLG (SL1)
- — GR SLG maintains status of main office, client stays at GR

- **Main office comes back**

  GR SLG redirects client to main office SLG

CS 1000 Release 7.0 compatibility matrix

For compatible applications that operate with CS 1000 Release 7.0 software, obtain the CS 1000 Release 7.0 product Bulletin or contact your Nortel distributor before upgrading. Compatibility information is also available to distributor partners through the Partner Information Center at www.nortel.com

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

Interoperability with other products

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

Table 6
Interoperability with other products

Product	Release
Call Server	
CS1000 N-1, N-3 CS1K	Release 4.5 and 5.5
CS2100 (SIP, H.323, PRI)	SE11
MCS5100/MAS	MCS 4.0
BCM50	Release 3.0
BCM450	Release 1.0
CS 2000	CVM11
Branch Office	
SRG50	Release 3.0
Applications	
ACE(Agile Communication Environment)	Release 1.1
MPS 500	3.0.0.15
MPS IP (ICP)	1.0.1.155
Contact Center	Release 6.0

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

Table 7
Release comparison summary

Auxiliary Processors	Succession Release 3.0	CS 1000 Release 4.0
Attendant consoles		
PC Attendant Console	1.2.x	1.2.x
M2250 Attendant Console	Supported	Supported
SMILE	2.3.x	2.3.x
Digital telephones		
M39xx	F/W version shipped with Release 3.0	F/W version shipped with Release 4.0
Meridian Modular Telephones (M2xxx)	Supported	Supported
ITG-P and Media Cards		
IP Line	3.1	4.0

Table 7
Release comparison summary (cont'd.)

Auxiliary Processors	**Succession Release 3.0**	**CS 1000 Release 4.0**
IP Trunk	3.00.53, 3.01.22, 3.01.60 (Will resolve with Signaling Server 2.10.81, 2.11.03, 4.00.xx.)	3.01.22, 3.01.60 (Will resolve with Signaling Server 2.11.03, 4.00.xx.)
System management		
Optivity Telephony Manager (OTM)	OTM 2.1 and OTM 2.2	OTM 2.2
Element Manager	Part of core Signaling Server software	Part of core Signaling Server software
Messaging		
CallPilot	1.07 (with Service Update 4), 2.0 Used on Platforms: 201i, 702t, 703t, 1001rp, 1002rp versions	1.07 (with Service Update 4), 2.0, 2.5 Used on Platforms: 201i, 702t, 703t, 1001rp, 1002rp versions
HMS 400	1.0	1.0
CallPilot Mini	1.5, 1.5A, 1.5B, 1.5C, 1.5D Small Systems only	1.5, 1.5A, 1.5B, 1.5C, 1.5D Small Systems only
Meridian Mail Modular Option EC	12.12-13.14	12.12-13.14
Meridian Mail Enhanced Card Option	12.12-13.14	12.12-13.14
Meridian Mail Reporter R2.X	Not dependent on core software	Not dependent on core software
Wireless		
Companion	3.xx -7.xx (7.xx required for Enhanced Capacity)	3.xx -7.xx (7.xx required for Enhanced Capacity)
Voice over Internet Protocol (VoIP)		
Meridian DECT (DMC4/DMC8 version)	451000.xx / 470001.xx – software embedded on IPE card	451000.xx / 470001.xx – software embedded on IPE card
VoIP – 802.11 Wireless IP Gateway with Symbol	Application supported on ITG Pentium only 1.1x	Application supported on ITG-P 24-port card 1.19, 1.20

Table 7
Release comparison summary (cont'd.)

Auxiliary Processors	**Succession Release 3.0**	**CS 1000 Release 4.0**
IP Phone 2001	Not supported	Firmware version shipped with Release 4.0
IP Phone 2002	Firmware version shipped with Release 3.0	Firmware version shipped with Release 4.0
IP Phone 2004	Firmware version shipped with Release 3.0	Firmwareversion shipped with Release 4.0
IP Phone 2002 Phase II	Not supported	Firmware version shipped with Release 4.0
IP Phone 2004 Phase II	Not supported	Firmware version shipped with Release 4.0
IP SoftPhone 2050	Firmware version shipped with SR3.0	Firmware version shipped with Release 4.0
WLAN Handset 2210/2211	Not supported	Firmware Release 97.039
IP Telephony Manager 2245	174.007	174.007
Remote office portfolio		
Remote Office 9150	1.3.1, 1.3.4, 1.4.x, 1.5.x	1.4.x, 1.5.x
Remote Office 9110/9115/ IP Adaptor	1.3.1, 1.3.4, 1.4.x, 1.5.x	1.4.x, 1.5.x
Meridian Home Office MHO-II	1.18 Not supported with M3900 Phase III	1.18 Not supported with M3900 Phase III
Mini Carrier Remote	Supported	Supported
Carrier Remote	Supported	Supported
Fiber I	Supported	Supported
Fiber II	Supported	Supported
Remote Peripheral Equipment (RPE)	Not supported	Not supported
Retired call center applications		
Meridian MAX (any platform)	(9.2, 9.3), 10.x	Not supported
Network Administration Center (NAC)	Not supported - End of Life Last release - 2.5	Not supported
Meridian Customer Controlled Routing (MCCR)	Not supported - End of Life Last release - 3B, 3C	Not supported

Table 7
Release comparison summary (cont'd.)

Auxiliary Processors	Succession Release 3.0	CS 1000 Release 4.0
Meridian Link (Mlink)	Not supported - End of Life Last release - 5, 5C	Not supported
Symposium Link	Not supported	Not supported
Symposium Desktop TAPI Service Provider for Meridian Communicator Adapter (MCA)	Not supported - End of Life Last release - 1.x - 2.x	Not supported
Meridian Link & MCCR Co-residency	Not supported	Not supported
Symposium Call Center and CTI applications		
Symposium Telephone Application Programming Interface (TAPI) Service Provider	2.3.1, 3.0	3.0
Symposium Agent	2.3	2.3
Symposium Agent Greeting	2.0	2.0
Nortel Remote Agent Observe	1.0	1.0
Meridian Link Services (MLS)	4.2	5.0
Symposium Express Call Center (SECC)	4.2	4.2
Symposium Call Center Server (SCCS) **ATTENTION** Includes Symposium Web Client	4.0, 4.2, 5.0	4.2, 5.0
Symposium Web Centre Portal (SWCP)	4	4.0
CTI.next (Nortel Networks Communications Control Toolkit)	5.0	5.0
IVR applications		
Periphonics IVR (VPS/is)	5.x	5.x
Periphonics Integrated Package for Meridian Link (IPML) – VPS/is and MPS	2.0.x, 2.1	2.0.4, 2.0.5, 2.1

Table 7
Release comparison summary (cont'd.)

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

Planning considerations for the network-wide upgrade

Contents

This chapter contains information on the following topics:

Introduction

This section describes what combinations of mixed software are allowed in a network running Communication Server (CS) 1000 Release 6.0. Mixed situations are likely to occur temporarily as the upgrade progresses.

Planning for a new platform

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

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

UCM

You can access a UCM server by using either FQDN or IP address.

If you access a UCM server through its FQDN, single sign-on is enabled and you can further navigate from one server to another from the UCM interface without logging in again.

If you access a UCM server through its IP address, single sign-on is not enabled. When navigating from one server to another from the UCM interface, the user must log in again to the target server.

Network Routing Service

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

It is possible to operate CS 1000 Release 7.0 nodes with CS 1000 Release 5.5 NRS for a short time if the upgrade logistics require this. Some new feature capability may not operate.

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

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

System and network level security

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

- “Security domain” (page 30)
- “Central and local authentications” (page 31)
- “Intra-System Signaling Security or IPsec” (page 31)
- “Datagram Transport Layer Security” (page 33)

Security domain

A security domain is a centrally managed collection of elements which includes call servers, signaling servers, media gateways, or media cards that belong to CS 1000 systems, as well as standalone servers. For example, a server running an NRS that operates at the network level. The centralized management functionality is implemented by a primary UCM security server (along with an optional secondary UCM security server).

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

Central and local authentications

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

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

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

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

Intra-System Signaling Security or IPsec

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

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

Two levels are supported for ISSS. The following table shows the definition for these levels:

Table 8
ISSS levels definition

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

Name	Description	Limitations	Level of security	Intended use
	the ELAN are denied without IPsec.	use IPsec. All other protocols are denied on the ELAN.		register the security domain using manual mode. System mode register will not be available.

ATTENTION
Before upgrading to CS 1000 Release 7.0, you need to manually disable ISSS on the system where it was previously used.

Datagram Transport Layer Security

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

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

The following table Table 9 "Security levels" (page 33) describes the security levels in detail:

Table 9
Security levels

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

	policy on the 7.0 systems is set to **DTLS Best Effort**			
Advanced Security	DTLS is enabled in all the systems in the network and are set to **DTLS Best Effort**	There cannot be any DTLS-incapable systems in the network.	Good	This security level is intended for customers who require more security. But they must use DTLS-incapable phones (such as Polycom conference phone 2033 or Wireless Phones 221x series).
Complete Security	All systems in the network are DTLS-enabled and set to **DTLS only**	There can be no DTLS-incapable equipment on the network, servers, or IP Phones. Connecting a phone with an old firmware version may require creating an isolated IP Telephony Node in a black LAN.	Best	This security level is intended for customers who require encryption of every bit of information on the network, such as military or government institutions.

Network Time Protocol configuration

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

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

When upgrading a CS 1000 system to CS 1000 Release 7.0 it is necessary to configure NTP settings using Element Manager (EM). Previous settings on the Call Server, such as external NTP clock sources, are extracted and presented as defaults. NTP configuration performed by EM is applied to all system elements. If this EM configuration of NTP is not performed, then NTP will not function correctly for the system.

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

Other Linux elements that are not part of a CS 1000 Release 7.0 system (for example, standalone NRS, standalone UCM primary security server) must be configured individually for NTP synchronization. These would normally point to external NTP clock sources. The UCM Base Manager of each element should be used for NTP configuration.

Deployment considerations

This section describes deployment options to consider for supported configurations:

- “Management of IP telephony nodes” (page 35)
- “Personal directory and unicode name directory” (page 36)
- “Primary and secondary NRSs” (page 36)
- “Element manager” (page 37)
- “Primary and secondary UCM security servers” (page 37)
- “Subscriber Manager” (page 38)
- “Survivable Remote Gateway” (page 38)

Management of IP telephony nodes

SIP line, UNIStim line TPS (LTPS), and virtual trunk (VTRK) applications running on the signaling servers in an IP telephony node are managed as a group. The signaling servers in a node are linked to a single call server, and an election is run to select a signaling server that acts as the leader and takes on the node IP address. There is only one set of configuration settings (node ID, call server IP address, TLAN node IP address and subnet mask, ELAN gateway IP address and subnet mask) per node.

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

There is no server level configuration for application services and it is applied on a Nodal level where all servers that belong to the Node share the same set of services.

The Node must have minimum one server as a Node element in order for that Node to be operational. The administrator can add as many servers to be part of the Node and all the Node elements will have the same set of application services enabled, however only one physical server can be active at a time. This active server can run all the configured services on that physical server, For example, UNIStim LTPS and SIP can all be configured and enabled on the same server. The LTPS application is an exception where several servers can run active instances of LTPS service. The LTPS application supports load sharing.

Personal directory and unicode name directory

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

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

Primary and secondary NRSs

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

In addition, the combined processing load of all the software packages running on the secondary server should be approximately equal to the combined processing load on the primary server. For example, it is not recommended to have a configuration in which the primary NRS is standalone and the secondary NRS is on a server that runs other signaling server applications. This is because the secondary NRS will not be able to handle the processing load of the primary NRS.

ATTENTION
Configuration of nodes can only be modified from the primary NRS.

Element manager

There is one element manager (EM) for each CS 1000 system. The Release 5.0 or 5.5 configuration of a server hosting multiple EMs to serve multiple CS 1000 Release 6.0 systems is no longer supported in this release. In general, TDM systems can be managed by command line without requiring EM (which needs to run on a Linux-based signaling server). However, EM is required to configure DSPs on the daughterboards if the system expands beyond one box (10 slots), as this configuration capability is not available through the command line.

Primary and secondary UCM security servers

The primary UCM security server provides:

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

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

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

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

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

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

Subscriber Manager

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

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

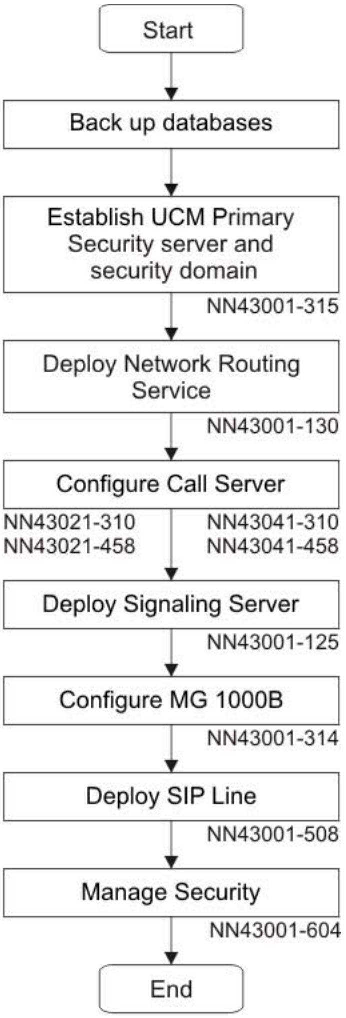
Survivable Remote Gateway

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

Upgrading the IP telephony network

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.

Figure 1
Steps for central upgrade



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

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

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

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

UCM

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

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

Complete upgrade to UCM

A single network UCM upgrade from Release 5.0, 5.5, or 6.0 to 7.0 must be carried out in a single maintenance window. Enter **`upgrade`** command from a 5.x Primary server's command line interface (CLI) to perform the upgrade. To upgrade the single system use the following steps:

Procedure 1
Linux Server Upgrade

Step **Action**

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

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

For example, in Release 6.0 both 'nortel' and 'admin' group have System admin privileges and can be used for upgrade.

For example, in Release 5.0 or 5.5 'nortel' group has System admin privileges and can be used for upgrade.

2 Type **`upgrade`** on the CLI.

```
[nortel@otm-ibm7 ~]$ upgrade


This tool will perform Linux Base upgrade.  Before the
upgrade it will back up all data.


Do you want to continue upgrade?  (Y/N) [N]?

y
```

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

```
System data will be saved at /admin partition.


Please use option "Re-use /admin partition" during
Linux Base installation.

Do you want to backup data to external source (USB/SFTP)
as well?  (Y/N) [Y]?

Backup started.  Please wait...

INFO - Initializing ThreadPoolExecutor

INFO - Result=Quantum backup restore completed
Successfully.  Status=Quantum back up restore
completed.

Backup complete.


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

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

ATTENTION

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

```
Existing Configuration Partition Usage

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

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

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

If this re-installation is not due to disk corruption,
then leaving the partition is a safe option, and if
valid data from the previous configuration exists, you
```

```
will be given the option of reusing that data during
this installation.

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

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

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

1
```

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

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

y
```

--End--

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

Procedure 2
Upload software to the deployment server

Step	Action

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

> **ATTENTION**
> You need to login to the primary even if you have upgraded a member server.

2 Click on the **software deployment** link.

3 Click on the **software loads** link in deployment manager (DM) to upload the application software.

4 In DM, from the targets page, select the server's radio button.

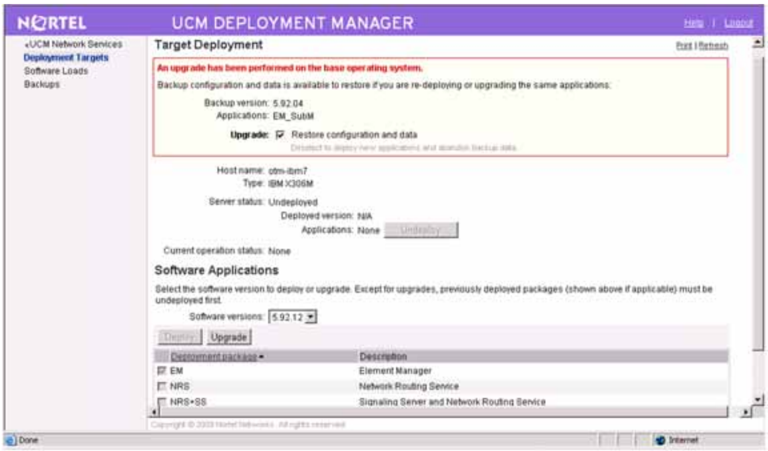
5 Click **Deploy**.

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

6

> **ATTENTION**
> If you are upgrading a CS 1000 Release 7.0 system, the packages are pre-selected as the previous deployment, and the **Upgrade** button is enabled.

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



Target Deployment

An upgrade has been performed on the base operating system.

Backup configuration and data is available to restore if you are re-deploying or upgrading the same applications.

Backup version: 5.92.04
Applications: EM_SubM

Upgrade: ☑ Restore configuration and data
Deselect to deploy new applications and abandon backup data.

Host name: cdm-ibm7
Type: IBM X306M

Server status: Undeployed
Deployed version: N/A
Applications: None

Current operation status: None

Software Applications

Select the software version to deploy or upgrade. Except for upgrades, previously deployed packages (shown above if applicable) must be undeployed first.

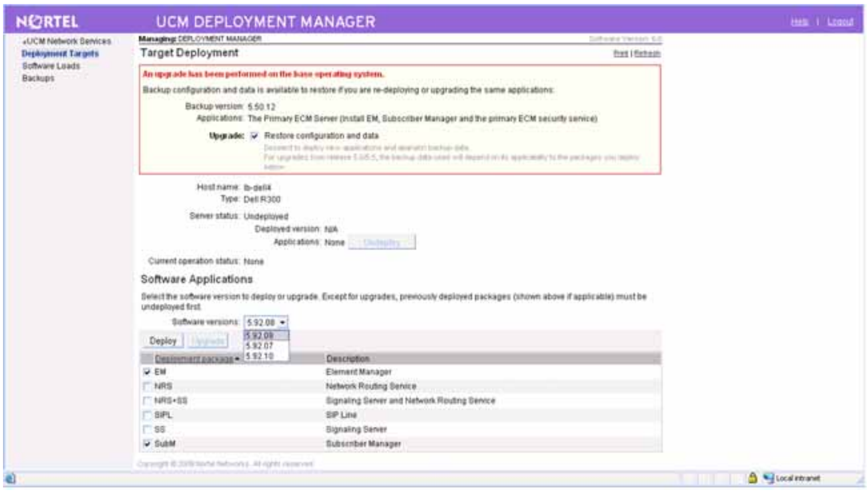
Software versions: 5.92.12

	Deployment package	Description
☑	EM	Element Manager
□	NRS	Network Routing Service
□	NRS+SS	Signaling Server and Network Routing Service

Copyright © 2009 Nortel Networks. All rights reserved.

7

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



Target Deployment

An upgrade has been performed on the base operating system.

Backup configuration and data is available to restore if you are re-deploying or upgrading the same applications:

Backup version: 5.50.12
Applications: The Primary ECM Server (install EM, Subscriber Manager and the primary ECM security service)
Upgrade: ☑ Restore configuration and data

Host name: lb-dell4
Type: Dell R300
Server status: Undeployed
Deployed version: N/A
Applications: None
Current operation status: None

Software Applications

Select the software version to deploy or upgrade. Except for upgrades, previously deployed packages (shown above if applicable) must be undeployed first.

Software versions: 5.92.08 (5.92.08, 5.92.07, 5.92.10)

Deployment package	Description
☑ EM	Element Manager
□ NRS	Network Routing Service
□ NRS+SS	Signaling Server and Network Routing Service
□ SIPL	SIP Line
□ SS	Signaling Server
☑ SubM	Subscriber Manager

Choose the software version to upgrade to.

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

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

--End--

Upon a successful upgrade, the manual security configuration is not required and the server is installed as a 6.0 Primary UCM Security server. The data from the 5.x server is restored.

Following are the details of data restore:

- Certificates -- None of the certificates and list of trusted certificate authentications (CAs) from the 5.x server are restored. The private key from the 5.x server's private CA are reused to create a new private CA for the 6.0 server.
- Roles -- All built-in and user defined roles are migrated. The permission mappings are lost. The permissions have to be mapped manually to the roles.
- Users -- All internal and external users are restored. The users will have the same role mapping as before. The default role for the user admin is Network administrator. In the 5.x database all user account passwords are hash encrypted. Hence they cannot be retrieved. As a result all users will have a default password "nortel12_Nortel".
- Elements -- UCM 6.0 does not support Release 5.0 and 5.5 CS 1000 application versions of EM, BCC, NRSM, and Subscriber Manager applications. Hence, none of the CS 1000 Release 6.0, NRSM, SIP

Gateway, and Subscriber Manager type elements are restored. The Element type for each element is converted to a 6.0 Hyperlink.

- Policies -- No user account and password policies are restored. They are set as per the defaults mentioned in 6.0. Information and configuration of External Authentication servers are not restored either.

Gradual upgrade to UCM from ECM

A mixed network is a network that contains CS 1000 Release 7.0 systems that are still running Release 6.0 or 5.5 and has been using ECM, then both ECM and UCM are required until the entire network is updated to CS 1000 Release 7.0. A mixed network UCM server upgrade must be performed when the entire 5.x ECM security domain can not upgraded to CS 1000 Release 7.0 at once. Networks running both CS 1000 6.0 and CS 1000 Release 7.0 must maintain two primary UCM servers. When all the systems are upgraded to 7.0, the 5.x or 6.0 primary COTS server can be removed from service and re-used.

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

Follow these steps to perform a mixed network upgrade:

Step	Action
1	Type nortel as the username to login to the CLI of the 5.x ECM Primary server.
2	Enter **`sysbackup -b`** command to generate a backup archive.
3	Install a CS 1000 Release 7.0 UCM server. The CS 1000 Release 7.0 UCM server should be fresh install without any reference to an existing backup file or configuration file.
4	Type nortel as the username to login to the UCM 6.0 server CLI.
5	Enter **`sysrestore`** command and select the backup file generated from the ECM 5.x server in step 1. The server is configured as a CS 1000 Release 7.0 Primary UCM security server. Only UCM specific data is restored from step 2.

--End--

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

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

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

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

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

Following are the details of data restore:

- Certificates -- The information required to bridge the trust between 5.x system and 6.0 system will be brought across by restoring the 5.x Primary backup data into the UCM 6.0 primary. The private key from the 5.x server’s private CA is reused to create a new intermediate private CA for the 6.0 server. As a result certificate details remains the same. The certificate start date refers to the current date and the certificate friendly name and common name refers to 6.0 server’s FQDN.
- Roles -- All built-in and user defined roles are migrated. The permission mappings are lost. The permissions have to be mapped manually to the roles.
- Users -- All internal and external users are restored. The users will have the same role mapping as before. The default role for the user admin is Network administrator. In the 5.x database all user account passwords are hash encrypted. Hence they cannot be retrieved. As a result all users will have a default password “nortel12_Nortel”.
- Elements -- The 6.0 UCM server acts as a launch point for all 5.x elements. All the 5.x elements are migrated to 6.0. The Element type for each element is converted to a 6.0 Hyperlink. You can not perform certificate related operations on the migrated elements.
- Policies -- No user account and password policies are restored. They are set as per the defaults mentioned in 6.0. Information and configuration of External Authentication servers are not restored either.

Following are the limitations in a mixed network:

- Single sign On -- System partially supports the Single Sign On between the 6.0 UCM network and the 5.x ECM network. Users are prompted for username and password only for the first time to launch a 5.x management application of a 5.x element. Thereafter the SSO cookie automatically authenticates any subsequent login, provided the user does not logout from the managed application or the session does not expire or terminate.
- Elements 5.x -- 5.x Elements cannot be added from the 7.0 Primary UCM server and vice-versa. Results of Edit and Delete operation carried out on a primary server will not reflect on the other. The changes made on the 5.x primary server decides the behavior of the Release 6.0 or 5.5 managed elements and changes made on the 7.0 primary server will decide the behavior of the CS 1000 Release 7.0 managed elements. The 7.0 UCM network acts as a unified launch point for all managed elements an administrator is concerned with.
- Users -- The roles mapped to the same user in 5.x server can be different from the mappings in the 6.0 server. Because some roles are no longer valid in CS 1000 Release 6.0. Also this causes the functional differences in 5.x and 6.0 environment.

NRS or SPS

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

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

It is possible to operate CS 1000 Release 7.0 nodes with CS 1000 Release 5.5 if the upgrade logistics require this.

The Linux SPS is part of the Linux NRS. For security certificates porting, it is part of UCM enhancement. The certificate is under UCM control. SIP GW and Linux NRS make use of this. You can export the certificate in the 5.5 or earlier Release and import them back into the CS 1000 Release 7.0.

ATTENTION

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

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

Procedure 3
Upgrading with a stand-alone NRS

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

--End--

Procedure 4
Upgrading with a co-located NRS

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

--End--

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

Survivable Remote Gateway

Survivable Remote Gateway (SRG) upgrades the IP Phone and redirects the IP Phone back to the CS 1000 Release 7.0. In order to interoperate with existing releases of the SRG, enable the FTP protocol on CS 1000 Release 7.0. As the FTP protocol is generally considered to be insecure, there is a tradeoff between the use of SRG and the amount of security provided by the system.

CS 1000M

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

CS 1000E

For CS 1000E CP PM system to convert from CS 1000 Release 7.0 CS 1000E CP PM call server (CS 1000) and CS 1000 Release 6.0 CP PM to a single CS 1000 Release 6.0 CS 1000E CS and signaling server Co-resident CP PM platform, the CP PM platform is converted to Linux based platform from Vxworks. The operations need to be done in the following order:

1. Upgrade Hardware (RAM and hard drive)
2. Upgrade BIOS and CP PM latest version
3. Install Linux base software
4. Install CS 1000 Release 7.0 and signaling server

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

For information on CS 1000 Release 7.0 and signaling server installation, see *Co-resident Call Server and Signaling Server Fundamentals* (NveN43001-509).

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

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

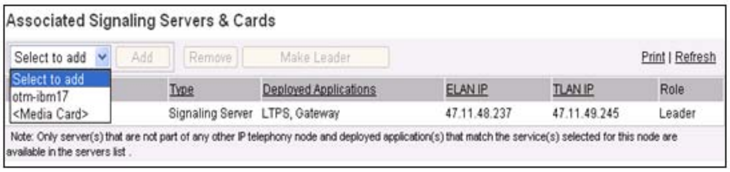
MG 1000E

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

Media cards

Follow these steps to install the media card:

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



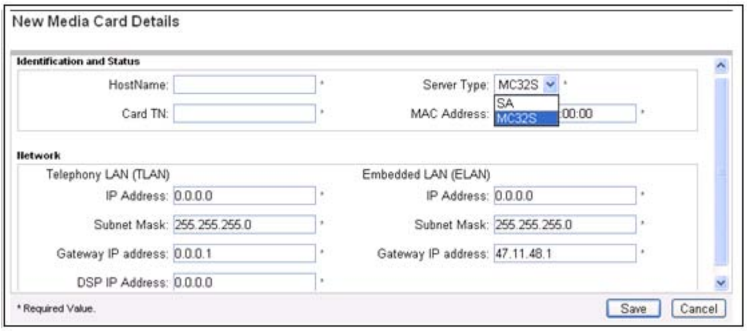
Associated Signaling Servers & Cards

Type	Deployed Applications	ELAN IP	TLAN IP	Role
Signaling Server	LTPS, Gateway	47.11.48.237	47.11.49.245	Leader

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list .

2 Enter the following attributes:

- Hostname
- Card TN
- Server Type
- MAC address
- ELAN and TLAN IP
- ELAN and TLAN Subnet Mask
- Card type
- DSP IP address



New Media Card Details

Identification and Status

HostName: *
Card TN: *
Server Type: MC32S *
MAC Address: :00:00 *

Network

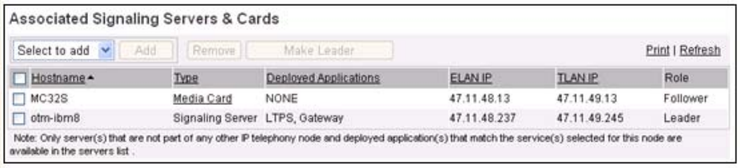
Telephony LAN (TLAN)
IP Address: 0.0.0.0 *
Subnet Mask: 255.255.255.0 *
Gateway IP address: 0.0.0.1 *
DSP IP Address: 0.0.0.0 *

Embedded LAN (ELAN)
IP Address: 0.0.0.0 *
Subnet Mask: 255.255.255.0 *
Gateway IP address: 47.11.48.1 *

* Required Value.

3 Click **Save** to return to Node edit page.

4 Save and Transfer the Node with the Media card configuration.



Associated Signaling Servers & Cards

□ Hostname▲	Type	Deployed Applications	ELAN IP	TLAN IP	Role
□ MC32S	Media Card	NONE	47.11.48.13	47.11.49.13	Follower
□ otm-ibm8	Signaling Server	LTPS, Gateway	47.11.48.237	47.11.49.245	Leader

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list .

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

--End--

Signaling server

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

MG 1000B

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

Security settings

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

Setting loadware

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

Index

Nortel Communication Server 1000

Planning the Network-wide Upgrade

Release: 7.0
Publication: NN43001-406
Document revision: 04.01
Document release date: 4 June 2010

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.

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

www.nortel.com