
Nortel Communication Server 1000

Nortel Networks Communication Server 1000 Release 4.5

System Redundancy

Document Number: 553-3001-307

Document Release: Standard 4.00

Date: July 2006

Copyright © 2006 Nortel Networks. All rights reserved.

Produced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, Nortel (Logo), the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Revision history

July 2006

Standard 4.00. This document is up-issued to include Nortel's recommendation that GRSEC package (405) be equipped during the software installation process (as per CR Q01356525). This note has been added to pages 20, 30, 50, 52, 62, 121, and 124.

April 2006

Standard 3.00. This document is up-issued to include Nortel's recommendation about enabling a switch of the CPP core processors during Daily Maintenance Routines (DROL).

August 2005

Standard 2.00. This document is issued to support Nortel Communication Server 1000 Release 4.5. This version contains numerous changes to campus redundancy.

September 2004

Standard 1.00. This document is issued to support Nortel Communication Server 1000 Release 4.0. Element Manager screens, Automatic NUID creation, and NRS routing are incorporated.

Contents

List of Procedures	11
About this document	13
Subject	13
Applicable systems	13
Conventions	14
Related information	15
Overview	17
Contents	17
Geographic Redundancy	17
Geographic Redundancy 1+1 configuration	18
Geographic Redundancy Controlled Load-sharing configuration	20
Geographic Redundancy N+1 configuration	22
Campus Redundancy	24
Geographic Redundancy 1+1 configuration	27
Contents	27
Description	28
Active Call Failover	30
Software	30
Hardware	31
Database replication	31
Normal operation	32
Redirection process	32

Primary system failure detection	37
Secondary system operating states	39
Secondary system failure	44
1+1 Planning	45
Planning the secondary system	45
Common CS 1000E and CS 1000M Large System planning considerations	46
Planning considerations specific to CS 1000E	49
Planning considerations specific to CS 1000M Large System (CP PII)	51
Numbering plan	54
Branch Office support	55
NRS Routing for Branch Office	57
1+1 configuration NRS routing example	59
Installing a 1+1 configuration	61
Configuring the primary system	64
Configure Backup Rule in LD 117	64
Configure Database Replication Control Block for Geographic Redundancy in LD 117	68
Configure Geographic Redundancy State Control Block in LD 117	71
Configuring primary (S1) and secondary (S2) Connect Servers . . .	75
Secondary system ACTIVE operation	75
Primary system recovery	77
Upgrades	79
Maintenance	80
OTM 2.2	80
Database configuration	80
Manual database replication and restore	81
1+1 Geographic Redundancy testing	86
1+1 system status	89
System faults	92
Network connectivity failure - call scenarios	93

Feature interactions	95
System monitoring	96
Limitations	96
Geographic Redundancy Controlled Load-sharing configuration	97
Contents	97
Description	98
Normal operation	99
Redirection process	100
Database configuration	101
Software	101
Hardware	102
Site 1 system failure	103
Site 2 system failure	105
Planning a Controlled Load-sharing configuration	106
Additional planning considerations	106
Network Bandwidth Management	110
Numbering plan	110
Branch Office support	112
NRS Routing for Branch Office	114
Installing a Controlled Load-sharing configuration	116
Provisioning the IP Phones	116
Maintenance	117
Feature interactions	118
System monitoring	118
Geographic Redundancy N+1 configuration	121
Contents	121
Description	121
Software	124
Planning	124

Campus Redundancy	127
Contents	127
Description	128
High Speed Pipe (HSP) IP address management enhancement	129
“Stop and Copy” protocol enhancement	129
Operating parameters	130
Normal Operations	130
Warmstart and Coldstart	131
Fault Detection	132
Switchover	133
Heartbeat	135
Network topology	135
Baystack 470 GBIC Fibre Interfaces	135
Campus Redundancy Baystack 470 Bandwidth Use	136
Switching Equipment	138
Call Server operation during IP network failure	140
ELAN subnet connectivity between the CPUs is lost but HSP is still operational	140
HSP connectivity is lost but ELAN subnet connectivity between the CPUs is operational	140
ELAN subnet and HSP connectivity is lost between the CPUs	141
HSP configuration	141
Initial installation	141
HSP recommendations and rules	141
High Speed Pipe IP address configuration	143
Customer validation	149
IP Telephony node configuration	149
Upgrading a redundant system	150
Downgrading a redundant system	152
HSP maintenance	153
STAT CPU	153
STAT HSP	156
STAT ELNK	157
Troubleshooting	158

Appendix A: Configuring the BayStack 470-24T for Campus Redundancy 159

Contents	159
Description	159
BayStack 470-24T configuration	161

Appendix B: Controlled Load-sharing zones 175

Contents	175
Network bandwidth management zones	175
Zone-based digit manipulation	176
Configuring zone parameters at the backup site	178
Element Manager zone configuration	184
Configuring zone parameters at the home site	186
Element Manager zone configuration on the home system	192
Configuring zone-based digit manipulation	193
Configuration example for PSTN resources	196

List of Procedures

Procedure 1	
Planning the secondary system	45
Procedure 2	
Installing 1+1 configuration	61
Procedure 3	
Configuring Backup Rule in Element Manager	66
Procedure 4	
Configuring Database Replication Control Block in Element Manager	70
Procedure 5	
Configuring Geographic Redundancy State Control Block in Element Manager	73
Procedure 6	
Clearing secondary system ACTIVE state in Element Manager	76
Procedure 7	
Recovering the primary system database	78
Procedure 8	
Testing the recovered primary system	79
Procedure 9	
Manually invoking the database replication in Element Manager	82
Procedure 10	
Manually invoking the database restore in Element Manager	84

Procedure 11
Performing 1+1 Geographic Redundancy testing in Element Manager87

Procedure 12
Performing Test Local Mode88

Procedure 13
Obtaining 1+1 system status in Element Manager ...92

Procedure 14
Installing Controlled Load-sharing configuration116

Procedure 15
Configuring the BayStack 470-24T using web-based management162

Procedure 16
Configuring ESN and redundant IP Phone zones178

Procedure 17
Configuring the home system zone187

Procedure 18
Configuring the zone-based digit manipulation193

About this document

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

Subject

This document provides the information necessary to plan, install, and configure system redundancy for CS 1000E systems and CS 1000M Large Systems.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M CH)
- Communication Server 1000M Cabinet (CS 1000M CA)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)

- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

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

Conventions

Terminology

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

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

The following systems are referred to generically as “Small System”:

- Communication Server 1000M Chassis (CS 1000M CH)
- Communication Server 1000M Cabinet (CS 1000M CA)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as “Large System”:

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Data Networking for Voice over IP* (553-3001-160)
- *Dialing Plans: Description* (553-3001-183)
- *Signaling Server: Installation and Configuration* (553-3001-212)
- *IP Peer Networking: Installation and Configuration* (553-3001-213)
- *Media Gateway 1000B: Installation and Configuration* (553-3001-214)
- *Features and Services* (553-3001-306)
- *Software Input/Output: Administration* (553-3001-311)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Software Input/Output: Maintenance* (553-3001-511)
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120)
- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000E: Planning and Engineering* (553-3041-120)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)

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.

Overview

Contents

This section contains information on the following topics:

Geographic Redundancy	17
Geographic Redundancy 1+1 configuration	18
Geographic Redundancy Controlled Load-sharing configuration ..	20
Geographic Redundancy N+1 configuration	22
Campus Redundancy	24

Geographic Redundancy

CS 1000M Large Systems (CP PII and CP PIV) and CS 1000E systems both provide redundancy using dual processors. This allows a system to remain operational following a local component failure.

Geographic Redundancy further increases the reliability of CS 1000M Large Systems (CP PII and CP PIV) and CS 1000E systems by providing a remote system to serve as a backup for a local system. The remote backup

ensures continued service for all IP Phones in case of a catastrophic failure (for example, as a result of floods or fire).

IMPORTANT!

Geographic Redundancy provides redundancy for IP Phones only. Geographic Redundancy for analog (500/2500-type) telephones and digital telephones is not supported. Analog (500/2500-type) and digital telephones can still be connected to a system, but they will not be operational if the system fails.

IMPORTANT!

The use of static SIP endpoints is unsupported and will not work. Dynamic endpoints are required so that the system recognizes the state of the endpoints.

Geographic Redundancy provides a number of flexible configurations to achieve the required reliability. Careful planning is required to determine the solution that is right for each installation.

The three main Geographic Redundancy configurations are as follows:

- 1+1 configuration
- Controlled Load-sharing configuration
- N+1 configuration

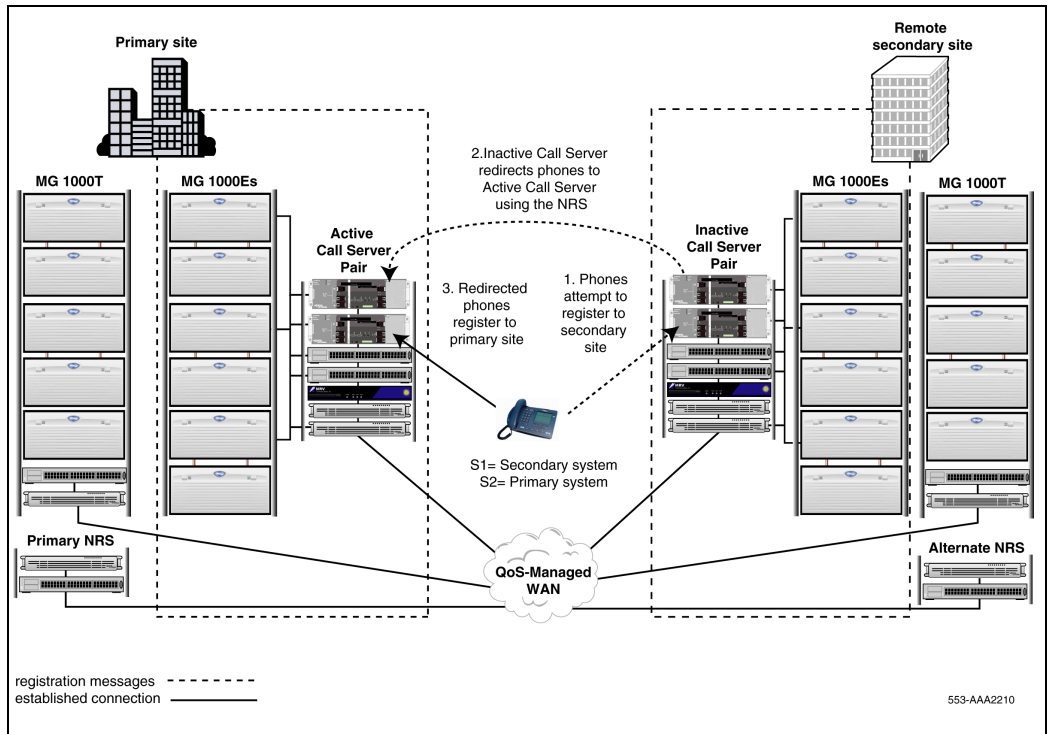
Geographic Redundancy 1+1 configuration

The Geographic Redundancy 1+1 configuration provides one secondary system that serves as a dedicated standby for a primary system. The secondary system becomes active only when the primary system fails.

With a 1+1 configuration, the primary and secondary systems must be the same type; that is, a CS 1000M is required to back up another CS 1000M system, and a CS 1000E system is required to backup another CS 1000E system.

Figure 1 shows a 1+1 configuration for a CS 1000E system.

Figure 1
1+1 configuration



In the 1+1 configuration, all IP Phones in the system are configured with their primary connect server (S1) pointing to the secondary system. When they power up, all IP Phones register with the secondary system. The secondary system then automatically redirects the IP Phones to the primary system for registration and normal operation.

If the primary system fails, the secondary system cannot successfully redirect the IP Phones. Therefore, the IP Phones remain registered with the secondary system to obtain continued service.

Two new software packages are introduced to support the 1+1 configuration: package 404 (GRPRIM) installed on the primary system and package 405 (GRSEC) installed on the secondary system. These packages are mutually exclusive and allow the customer database on the primary system to be regularly replicated to the secondary system across the Wide Area Network (WAN).

Note: The GRSEC package (405) must be equipped during the software installation process; it cannot be added using a new keycode post software installation.

For more details on the 1+1 configuration, see “Geographic Redundancy 1+1 configuration” on page 27.

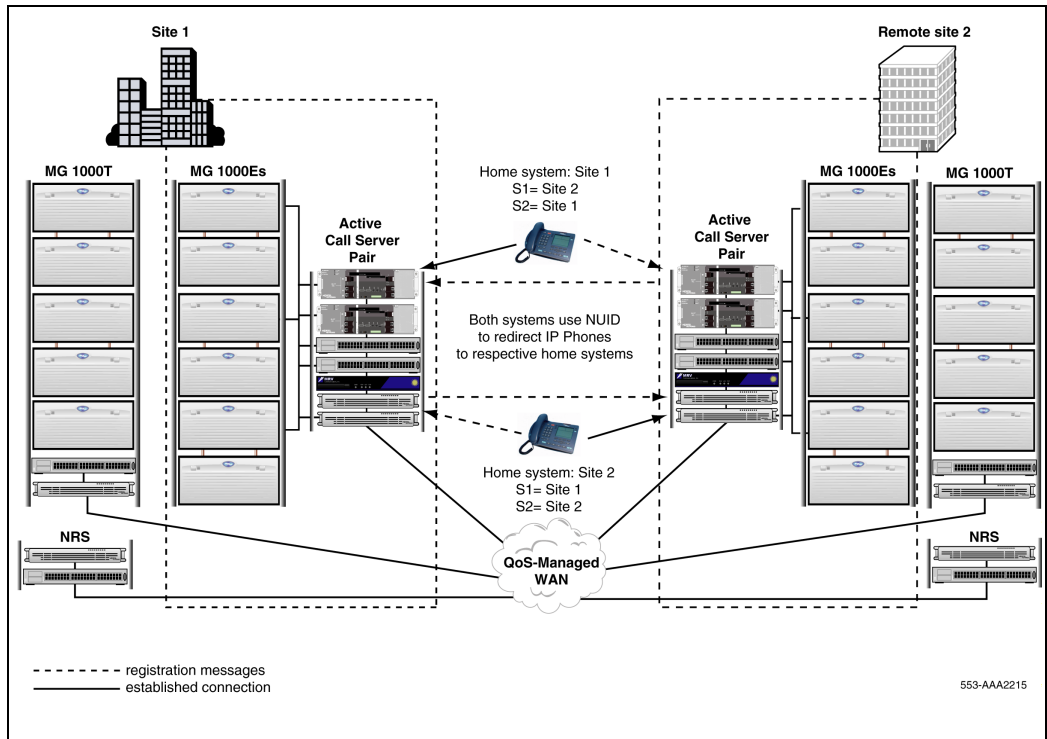
Geographic Redundancy Controlled Load-sharing configuration

The Controlled Load-sharing configuration also provides additional system redundancy, but unlike the 1+1 configuration, it does not require a dedicated standby backup system. Instead, it allows active systems in a network to provide the necessary redundancy for one another.

The Controlled Load-sharing configuration can be implemented using different system types. A CS 1000M Large System can back up a CS 1000E system, and a CS 1000E system can back up a CS 1000M Large System.

Figure 2 shows a Controlled Load-Sharing configuration for two CS 1000E systems.

Figure 2
Controlled Load-sharing configuration



The Controlled Load-sharing configuration employs similar functionality to the Branch Office feature. (See *Media Gateway 1000B: Installation and Configuration* (553-3001-214) for details.) For each IP Phone, a Directory Number (DN) and Terminal Number (TN) must be configured on a home system, where the IP Phone ultimately registers. On the backup system, the IP Phone is also assigned a DN and TN. This ensures that the backup system can provide the necessary functionality in case of failure at the home system.

On the backup system, each IP Phone is also assigned a Network User ID (NUID) and Network Home TN (NHTN), similar to the Branch User ID

(BUID) and Main Office TN (MOTN). The NHTN corresponds to a home system TN and the NUID corresponds to a dialable home system DN where the IP Phone ultimately registers. The backup system uses the NUID value in order to redirect IP Phones to the home system for registration.

Each IP Phone in the network is configured with its primary connect server (S1) pointing to its backup system. The backup system uses the defined NUID values to redirect each IP Phone to its home system for registration and normal operation. If the home system fails, the IP Phones remain registered on their backup system and receive service as normal.

For more details, see “Geographic Redundancy Controlled Load-sharing configuration” on page 97.

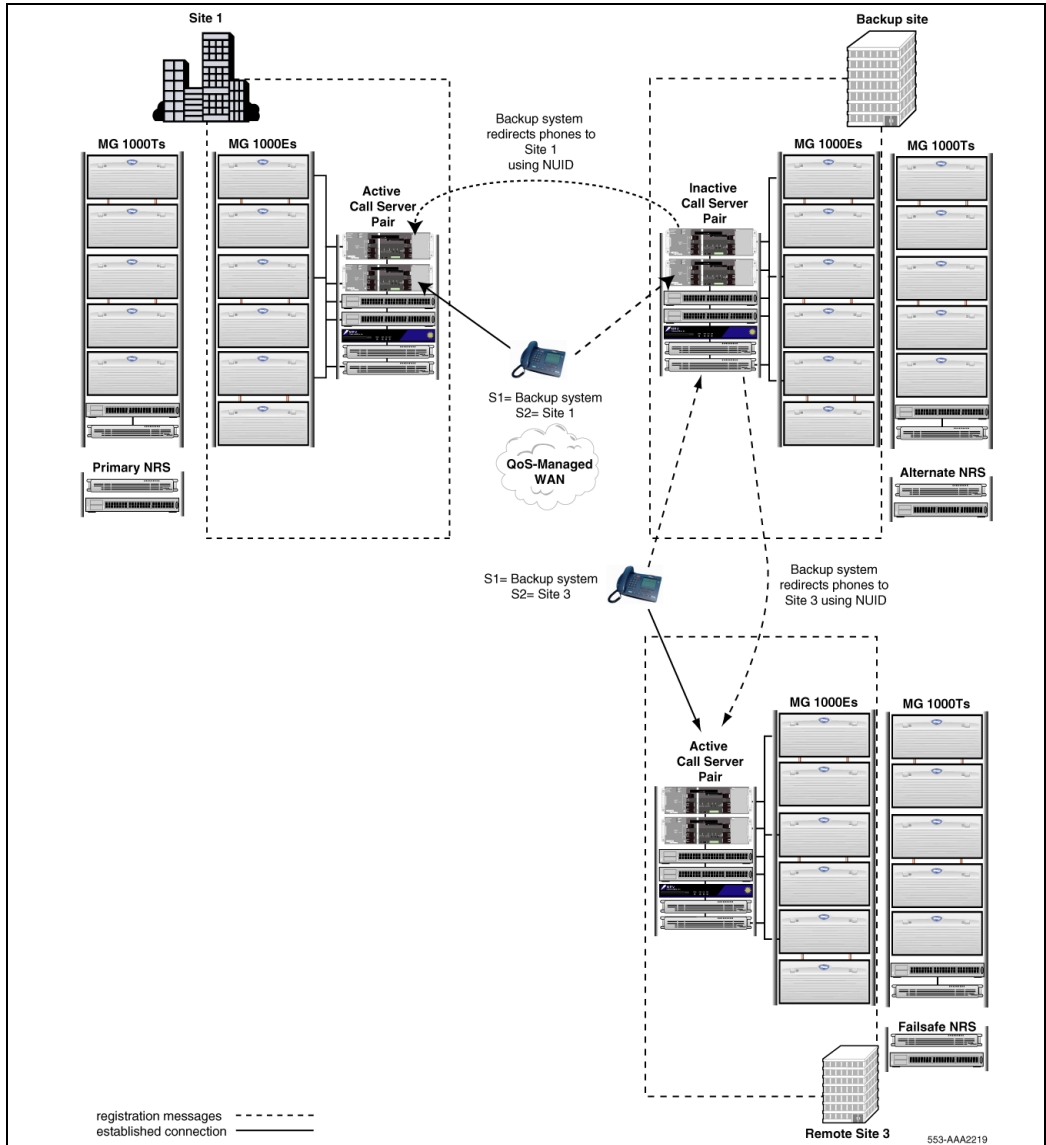
Geographic Redundancy N+1 configuration

The N+1 configuration increases the reliability of CS 1000M Large Systems and CS 1000E systems through the use of a geographically remote system that operates as a backup for multiple systems. The backup system assumes control of the affected IP Phones only when a home system fails.

The N+1 configuration can be implemented using different system types. A CS 1000M Large System can back up CS 1000E systems, and a CS 1000E system can back up CS 1000M Large Systems.

Figure 3 shows an N+1 configuration for CS 1000E systems.

Figure 3
N+1 configuration



In the N+1 configuration, each IP Phone in the network is configured with its primary connect server (S1) pointing to the backup system. The IP Phone therefore registers with the backup system at startup. The backup system then automatically redirects the IP Phone to its home system for registration and normal operation.

If either home system fails, the backup system assumes control of the affected IP Phones and provides the necessary services with a minimum impact on functionality.

For more details on the N+1 configuration, see “Geographic Redundancy N+1 configuration” on page 121.

Campus Redundancy

While Geographic Redundancy uses separate remote systems to provide the necessary functionality, Campus Redundancy increases the redundancy of a CS 1000E system through the physical separation of the CS 1000E Core Call Servers. It allows the remote standby Call Server to assume system control if the active Call Server fails.

Note: Campus Redundancy is not supported for CS 1000M Large Systems.

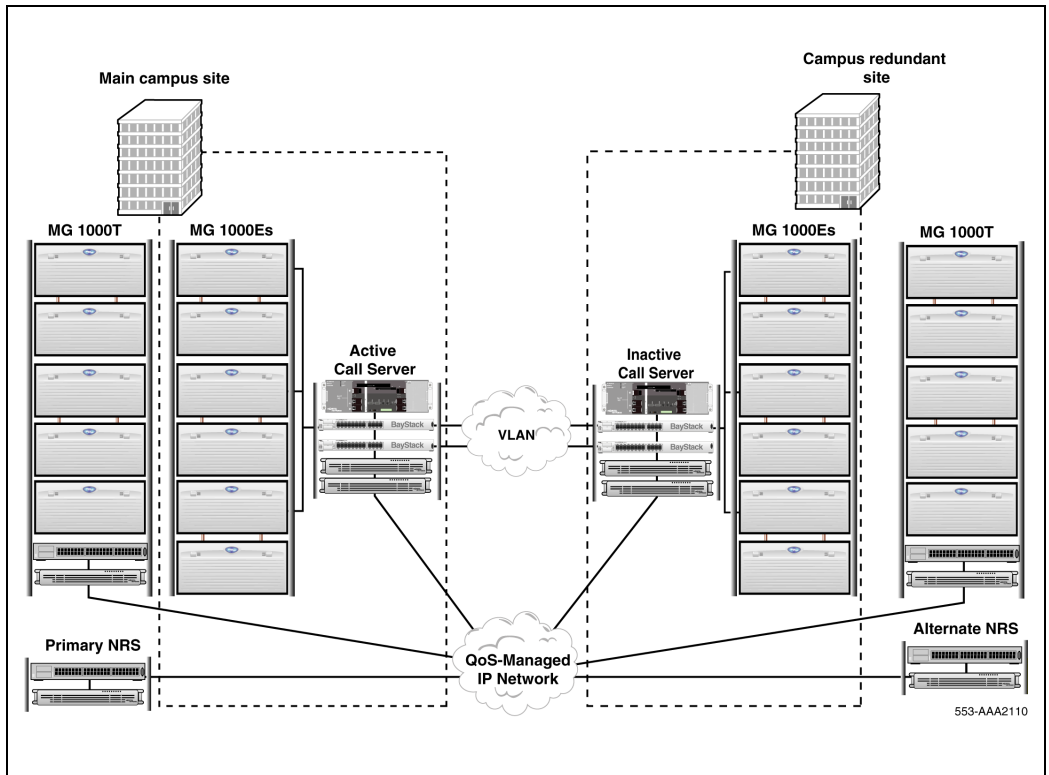
The Campus Redundancy feature provides the ability to separate the CS 1000E Call Servers in a campus environment for “campus mirroring”. This feature enables two Call Servers, one active and one redundant, to be connected through an Ethernet network interface. CS 1000 Release 4.5 provides enhancements to the CS 1000E system to allow campus mirroring to operate using a number of additional Layer 2 switching products, in addition to the BayStack 470.

To separate the redundant Call Servers, the ELAN subnet and the subnet of the High Speed Pipe (HSP) can be extended between the two processors with Ethernet switches. using Layer 2 protocol.

If the two Call Servers are collocated, they can be connected using a standard CAT5e or CAT6 crossover cable, limited to 100 meters in length.

Figure 4 illustrates the separation of the Call Servers using the Campus Redundancy feature.

Figure 4
Campus Redundancy



For more details on Campus Redundancy, see “Campus Redundancy” on page 24.

Geographic Redundancy 1+1 configuration

Contents

This section contains information on the following topics:

Description	28
Normal operation.....	32
Primary system failure detection.....	37
Secondary system failure	44
1+1 Planning	45
Numbering plan.....	54
Branch Office support.....	55
1+1 configuration NRS routing example	59
Installing a 1+1 configuration.....	61
Configuring the primary system	64
Secondary system ACTIVE operation	75
Primary system recovery.....	77
Upgrades	79
Maintenance	80
System faults	92
Network connectivity failure - call scenarios	93
Feature interactions	95
System monitoring	96

Limitations 96

Description

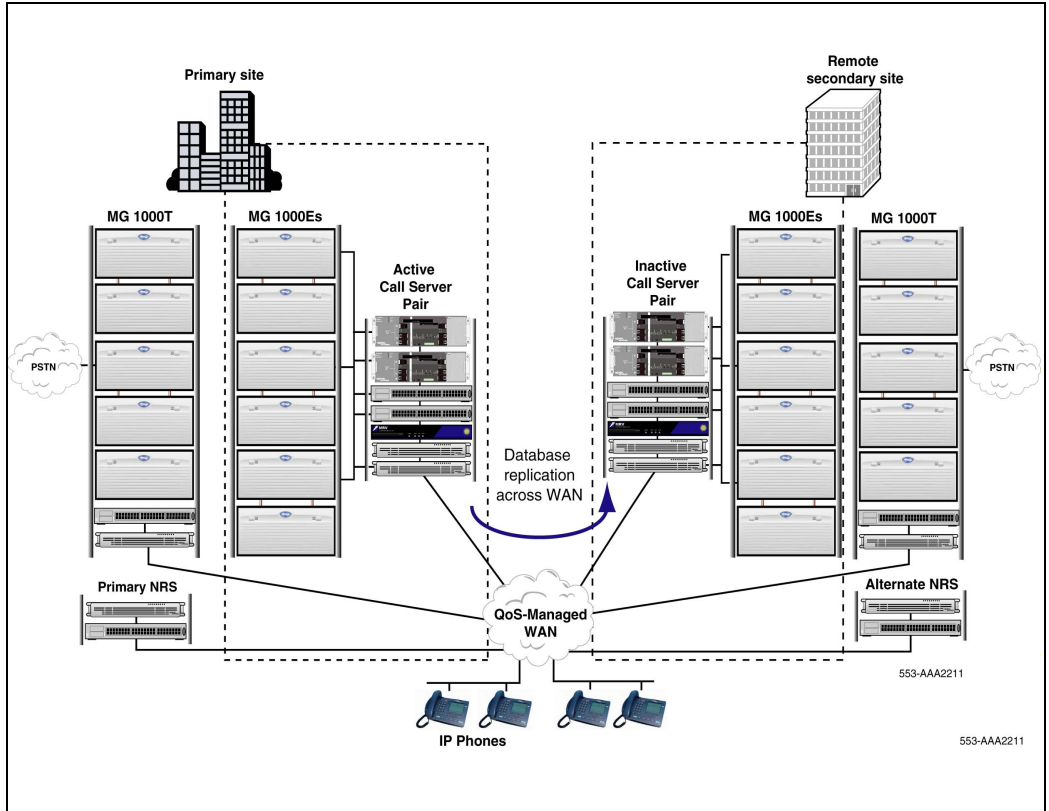
The 1+1 configuration increases the reliability of CS 1000M Large Systems (CP PII and CP PIV) and CS 1000E systems through configuration of a geographically remote system that provides the functionality required in the case of primary system failure. The secondary system becomes active only when a failure occurs at the primary site or when IP Phones cannot connect to the primary system due to network failure.

The secondary system database is replicated from the primary system database. As a result, the secondary system must be the same type of system as the primary system. That is, a CS 1000M Large System can be backed up only by another CS 1000M Large System and a CS 1000E system can be backed up only by another CS 1000E system.

Note: The 1+1 configuration provides redundancy for IP Phones only. Redundancy for analog (500/2500-type) telephones and digital telephones is not supported. Analog (500/2500-type) and digital telephones can still be connected to a primary system, but they will not be operational if the system fails.

Figure 5 shows a 1+1 configuration for CS 1000E systems.

Figure 5
1+1 configuration



Connectivity between the primary system and the secondary system is provided through a Quality of Service (QoS)-managed WAN.

Note: As it operates independently of the CS 1000E Core Call Servers, the Media Gateway 1000T (MG 1000T) platform is not encompassed by the 1+1 configuration. The MG 1000T can be collocated with the primary and secondary systems for convenience. However, provided the MG 1000T is operational, it remains available to both systems at all times.

Active Call Failover

CS 1000 Release 4.5 introduces the Active Call Failover feature. Active Call Failover ensures that active calls are not dropped during switchover.

For more information on Active Call Failover, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Software

To implement the 1+1 configuration, package 404 (GRPRIM) must be equipped on the local primary system, and package 405 (GRSEC) must be equipped on the remote secondary system. These two software packages are mutually exclusive.

Note: Package 404 (GRPRIM) is included on all CPP systems with a minimum service level of 2 except CPP systems equipped with package 405 (GRSEC).

Other than packages 404 and 405, the software packages on the secondary system must provide the same functionality as those offered on the primary system. Any attempted configuration differences on the secondary system are overwritten by the database replication.

The two systems must run CS 1000 Release 4.0 or later and must run the same software version, issue, and subissue.

Different software keycodes are required for the primary system to install the GRPRIM package and for the secondary system to install the GRSEC package. Other than these two packages, each keycode is configured to provide exactly the same functionality (such as system type, License limits, and software packages).

Note: The GRSEC package (405) must be equipped during the software installation process; it cannot be added using a new keycode post software installation.

Hardware

In the 1+1 configuration, the secondary system hardware must provide the same basic functionality as the primary system.

The simplest way to achieve full redundancy is to configure the primary and secondary systems with identical hardware configurations: the same circuit cards installed in the same slots and the same number and configuration of Signaling Servers.

However, as the secondary system provides redundancy for IP Phones only, digital and analog line cards are not required at the secondary site. As well, if the secondary system does not require the same capacity as the primary system, it is unnecessary to duplicate all of the primary system's physical components.

If the secondary system is not an exact duplicate of the primary system, ensure the secondary system can provide sufficient redundancy. For further planning details, see "1+1 Planning" on page 45.

Database replication

To ensure that the secondary system can provide the necessary functionality, configure the primary system in LD 117 to regularly replicate its database across the WAN to the secondary system. Database replication can be configured to occur automatically after each customer data dump in LD 43 and during the scheduled data dump at midnight.

Note: The automatic midnight data dump in LD 43 runs only when changes in the current database occur.

During each database replication, the primary system performs the following:

- 1 Makes a copy of the database backup files to a temporary directory on its hard drive.
- 2 Uses TAR utility to group this directory into one file.
- 3 Uses GZIP utility to compress the file.
- 4 Transfers the compressed file to the secondary system hard drive using FTP across the WAN.

To complete the replication process, the secondary system must perform a restore operation on the database received from the primary system. This operation is similar to the existing restore process from a floppy disk.

System-specific data is included in the replicated database, but is not restored to the secondary system. This data is defined separately on the primary and secondary systems (for example, IP addresses, netmasks, routes, and the Event Preference Table [EPT]).

Configure the secondary system to automatically initiate the restore operation once it receives a complete backup file. Once the restore operation is successful, the system must then perform a sysload to endorse the replicated primary system database. The sysload can also be configured to occur automatically.

Note: A predefined number of the previously transferred database versions are saved on the secondary system. If the automatic data endorsement fails, the database is automatically swapped with the previous database, and a new sysload is performed.

For more information on configuring the primary and secondary systems for automatic database replication, refer to “Installing a 1+1 configuration” on page 61.

Normal operation

Redirection process

In the 1+1 configuration, all IP Phones in the system must be configured with their primary Connect Server (S1) pointing to the secondary system node Terminal Proxy Server (TPS). When the IP Phones are reset, they attempt to register with the secondary system. The secondary system accepts these registration requests, but then automatically redirects all IP Phones to the primary system for registration.

IP Phones remain registered on the secondary system only if this redirection process fails due to a failure at the primary site or as a result of network connectivity failure.

Automatic NUID

To perform the redirection to the primary system, the secondary system automatically generates a Network User ID (NUID) for each IP Phone that it registers. The NUID is similar to the Branch User ID (BUID) that is used in the Branch Office feature for the redirection of IP Phones to a main office (see *Media Gateway 1000B: Installation and Configuration* (553-3001-214)). However, unlike the BUID in Branch Office (or the NUID in the Controlled Load-sharing configuration), the NUIDs in the 1+1 configuration are generated automatically, rather than manually.

To automatically generate the NUID, the secondary system uses the following formula:

$$\text{Automatic NUID} = (\text{AC1 or AC2}) + \text{HLOC} + \text{DN}$$

Table 1 describes in greater detail the logic used by the secondary system when it generates the NUID.

Table 1
Logic of the automatic generation of NUID (Part 1 of 2)

Variable	Logic
AC1 or AC2	In LD 15, Customer Data block, if LOC is associated with AC2, then the secondary system uses AC2 to build the NUID. Otherwise, it uses AC1. Values for AC1 or AC2 are defined in LD 86. (See <i>Software Input/Output: Administration</i> (553-3001-311) for details.)

Table 1
Logic of the automatic generation of NUID (Part 2 of 2)

Variable	Logic
HLOC	<p>The secondary system generates the NUID using the value of HLOC as defined in LD 15.</p> <p>(The same HLOC must be configured in LD 90 for the appropriate AC1 or AC2. See <i>Software Input/Output: Administration</i> (553-3001-311) for details)</p>
DN	<p>To choose the DN value for the NUID, the secondary system scans the IP Phone's keys, beginning from key 0 to its last key. The scan is stopped when a key with any of the following functions is met: ACD, MCN, MCR, PVN, PVR, SCN or SCR.</p> <p>The DN associated with the key is then used to generate the NUID. If no DN meets this criteria, the NUID cannot be generated.</p> <p>Note: For ACD (Automatic Call Distribution) key, the ACD DN or Message Center DN is used to generate the NUID.</p>

To generate the NUID, the secondary system uses values originally defined on the primary system. These values are copied to the secondary system during the database replication process. The NUID is therefore created with the HLOC value originally defined on the primary system. The secondary system can therefore use the NUID value to query the Network Routing Service (NRS) and determine the location of the primary system.

Note: To ensure that the IP Phone redirection is successful, the HLOC value for the primary system endpoint must be defined on the NRS as the least-cost route. (See "Numbering plan" on page 54 for details.)

The following provides a summary of the IP Phone redirection process from the secondary system to the primary system:

- 1 An IP Phone resets and, using its S1 value, registers first with the secondary system node Terminal Proxy Server (TPS), then with the secondary system itself.
- 2 The secondary system accepts the registration, then automatically generates the NUID for the registered IP Phone.

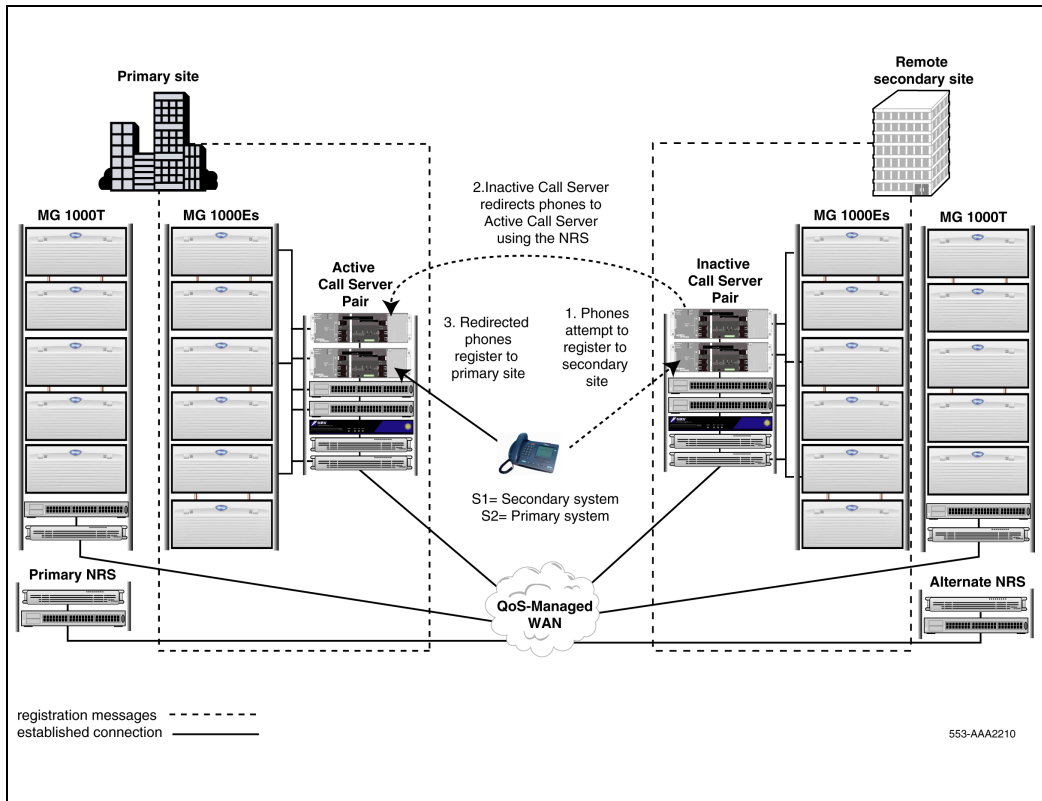
- 3 The secondary system TPS queries the NRS for the home system node indicated by the generated NUID.
- 4 The NRS responds with the least-cost route for the HLOC of the NUID (the primary system HLOC must be configured as the least-cost route).
- 5 When the secondary system receives the positive response, it redirects the IP Phone to the primary system.
- 6 The redirected IP Phone registers to the primary system.

Note 1: The NUID is used in the 1+1 configuration for redirection purposes only. When the IP Phone registers on the primary system, it uses the DN values that are defined on the primary system.

Note 2: Due to the database replication process, the TN of the IP Phone is the same on both primary and secondary systems. Therefore, a Network Home TN (NHTN) does not have to be defined in LD 11 for the IP Phones in a 1+1 configuration (for details on NHTN, see “Geographic Redundancy Controlled Load-sharing configuration” on page 97).

Figure 6 shows the normal IP Phone registration attempt and redirection process in a 1+1 configuration.

Figure 6
Normal operation



When both primary and secondary systems remain operational, all IP Phones are redirected by the secondary system and register with the primary system. The primary system provides service to all IP Phones.

The secondary system redirection also provides a practical means to monitor the network connections between the IP Phones, the primary system, and the secondary system.

While S1 points to the secondary system, all IP Phones must have their secondary Connect Server (S2) pointing to the primary system. This ensures that the IP Phones can register directly to the primary system and continue normal operations if the connection to the secondary system is lost.

Primary system failure detection

In the 1+1 configuration, the transfer of system control from a failed primary system to the secondary system is not a traditional switchover operation.

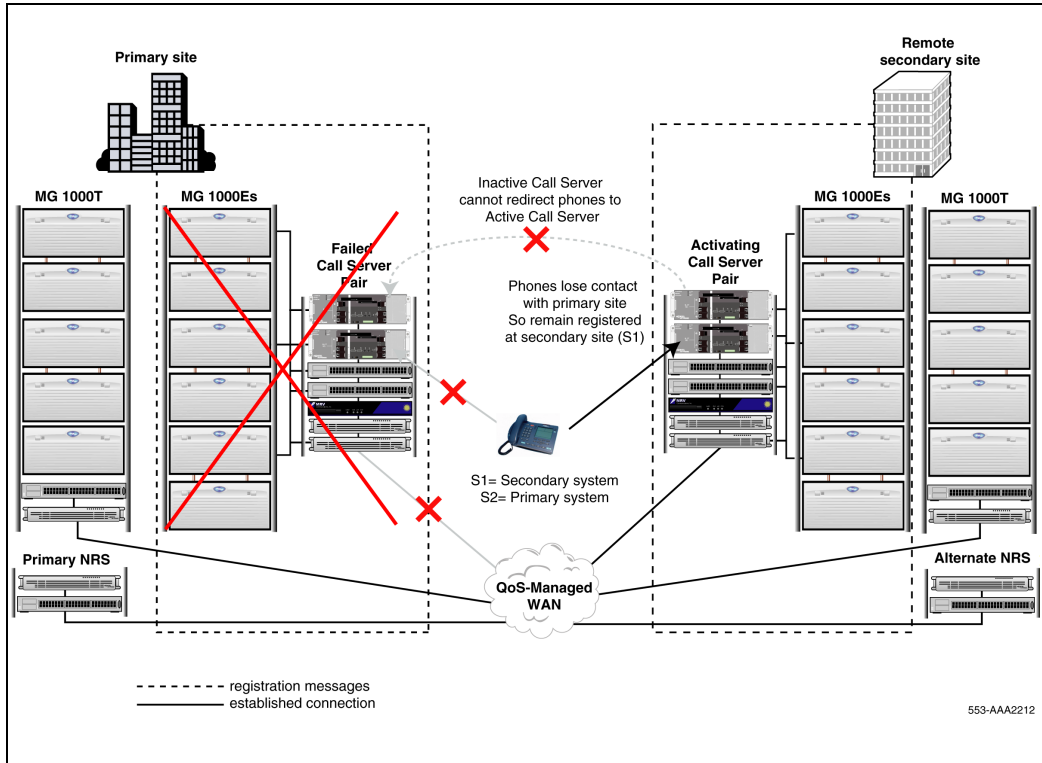
If the secondary system cannot redirect the IP Phones to the primary system because of a primary system failure (or network connectivity problem), the IP Phones stay registered on the secondary system. Therefore, each additional IP Phone that remains registered on the secondary system represents a potential problem with the primary system.

Note: Failure of the IP Phone to register to the primary system is not necessarily caused by a failure of the primary system. The cause can also be LAN/WAN connectivity problems. Geographic Redundancy does not differentiate between these types of failures.

To monitor primary system health, the secondary system maintains a real-time count of IP Phones (N) registered on the secondary system. Once the number of IP Phones (N) registered on the secondary system exceeds the Geographic Redundancy Threshold (GRTHR), the secondary system escalates to ACTIVATING state. (The customer can define GRTHR in LD 117.)

Figure 7 shows a primary site failure in a 1+1 configuration.

Figure 7
1+1 configuration: system failure at primary site



While in the ACTIVATING state, the secondary system provides the IP Phones with necessary service, but does not become fully active. This allows the secondary system to take into account a short-term failure at the primary site.

If the primary system regains full operation within a short period of time, as defined by the Short Term Failure Timer (STFT), the secondary system redirects all IP Phones to the primary system, and normal operation resumes.

Only when the primary system remains out-of-service past the STFT does the secondary system escalate to the ACTIVE state. This ensures that the ACTIVE state operating license period is not used unnecessarily.

Note: The secondary system ACTIVE state is limited by an operating license period of 90 days.

Secondary system operating states

The secondary system provides a number of operating states that allow it to transition smoothly from INACTIVE to ACTIVE and back again. Refer to Figure 8 on [page 40](#) and Table 2, “Secondary system state control data set,” on page 41 for a description of the secondary system state logic and the data set, including timers, that control the transitions between the various secondary system states.

Figure 8
Secondary system operating state logic

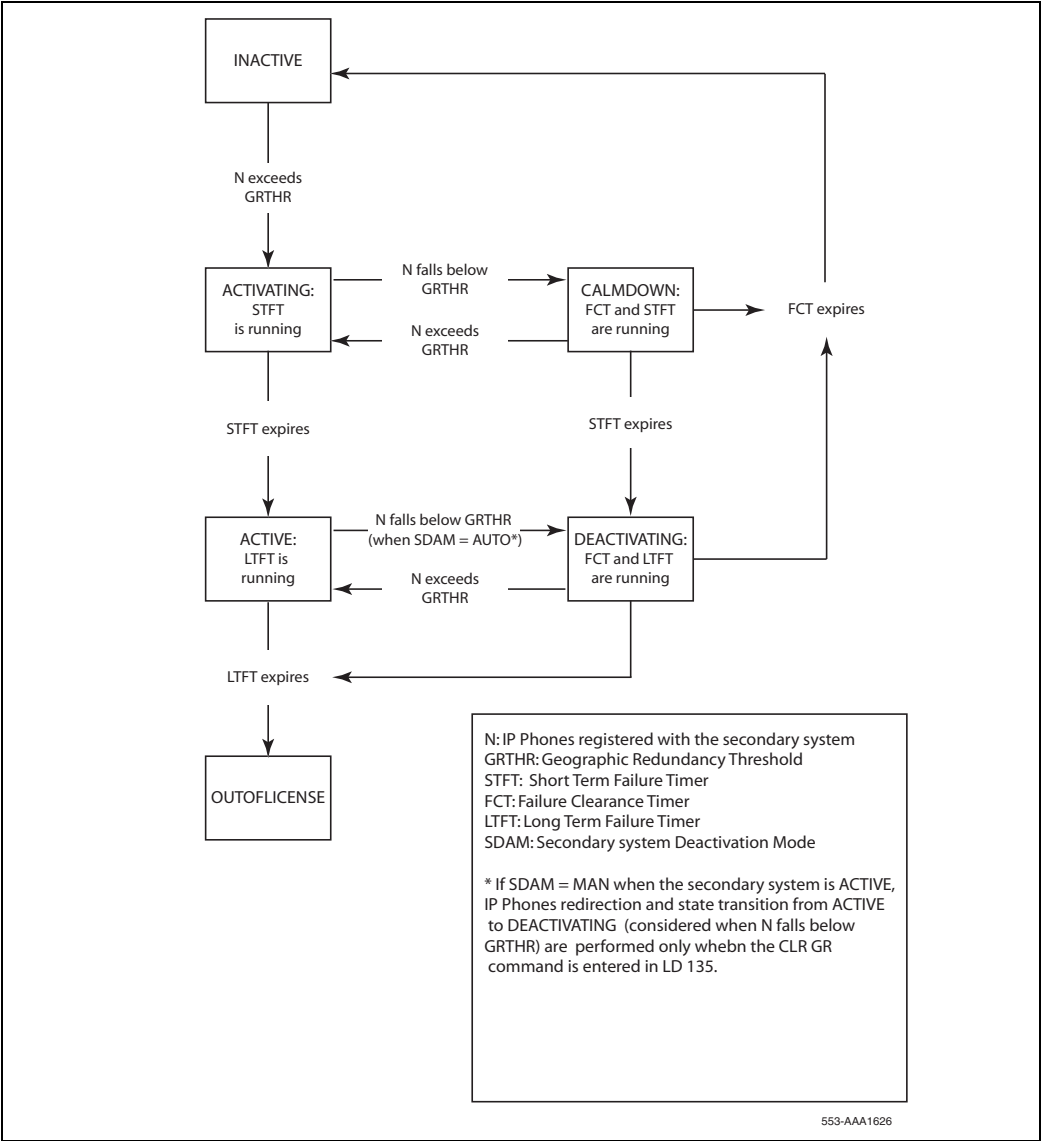


Table 2
Secondary system state control data set (Part 1 of 2)

Variable	Definition
N	Number of IP Phones registered with the secondary system, updated in real time. The secondary system uses this value to monitor primary system health.
GRTHR	Geographic Redundancy Threshold: a customer-definable threshold against which N is compared. If the secondary system is INACTIVE and N exceeds the GRTHR, the secondary system escalates to the ACTIVATING state. (GRTHR is configurable in LD 117.)
STFT	<p>Short Term Failure Timer: the short period of time during which the primary system can remain inoperable without the secondary system assuming full system control (for example, as caused by initialization, sysload, or minor technical failure).</p> <p>STFT starts when the secondary system enters the ACTIVATING state (N exceeds GRTHR). If the STFT expires while the system is in the ACTIVATING state, the secondary system escalates to the ACTIVE state. (STFT is configurable in LD 117.)</p>
FCT	<p>Failure Clearance Timer: period of time that must elapse once the primary system is brought back online (and N falls below GRTHR) before the secondary system state can revert to INACTIVE.</p> <p>This timer serves to prevent unnecessary transitions between less severe and more severe states when the value of N is close to GRTHR. (FCT is configurable in LD 117.)</p> <p>Note: FCT is also used with the CLR GR command in LD 135. FCT defines the period of time during which redirection attempts to the primary system are allowed.</p>

Table 2
Secondary system state control data set (Part 2 of 2)

Variable	Definition
LTFT	Long Term Failure Timer: license period during which the secondary system is allowed to run in the ACTIVE state. (LTFT is a hardcoded value of 90 days. It is not a customer-configurable value.) When LTFT expires, the system enters the OUTOFLICENSE state.
SDAM	<p>Secondary system Deactivation Mode: specifies whether the secondary system is in automatic deactivation (AUTO) or manual deactivation (MAN) mode.</p> <p>If SDAM = AUTO, the secondary system, once ACTIVE, queries the NRS for the primary system address every ten minutes. When the primary system comes back online the secondary system can resume the redirection of IP Phones to the primary system and automatically revert to the DEACTIVATING state (when N falls below GRTHR).</p> <p>If SDAM = MAN, the secondary system, once ACTIVE, stops trying to redirect IP Phones to the primary system. It stays in the ACTIVE state until the CLR GR command is initiated manually in LD 135. The CLR GR command triggers the redirection attempts to the primary system to resume (for a maximum period defined by FCT). If the redirections are successful and N falls below GRTHR, the secondary system reverts to the DEACTIVATING state.</p> <p>(SDAM is configurable in LD 117)</p>

For details on configuring the Geographic Redundancy State Control Block, refer to “Configure Geographic Redundancy State Control Block in LD 117” on page 71.

For details on the recovery of the primary system following a Long-Term Failure, refer to Procedure 7 on [page 78](#).

Secondary system operating state survival

The secondary system operating state can survive an initialization or a sysload (the operating state is restored from non-volatile memory). However, if the operating state is restored to ACTIVE after a sysload or initialization, the state transition from ACTIVE to DEACTIVATING is prevented for a period of 15 minutes. This waiting period eliminates unnecessary state

transitions as it allows the IP Phones to re-register to the secondary system. The secondary system can then obtain the appropriate value of IP Phones registered (N).

OUTOFLICENSE state

When the secondary system remains in the active state beyond the LTFT of 90 days and enters the OUTOFLICENSE state, some functional limitations are imposed on the secondary system. `Beyond licensed period` displays on all IP Phones and `Licensed period is exceeded` appears on the TTY banner upon successful login.

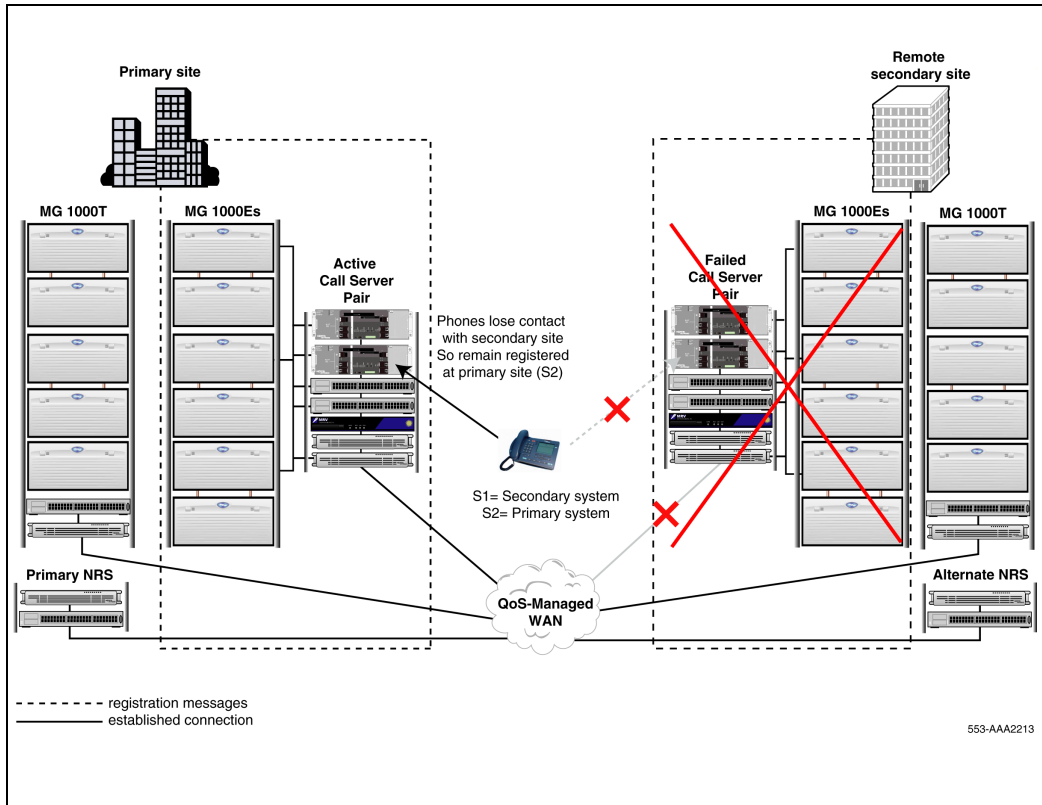
As well, all the data dump (midnight and manual), automatic restore, and automatic sysload operations are restricted.

To clear the OUTOFLICENSE state, a software installation is required.

Secondary system failure

Figure 9 shows a secondary site failure in a 1+1 configuration.

Figure 9
1+1 configuration: system failure at secondary site



If the secondary system fails while the IP Phones are registered on the primary system, the primary system continues to provide normal telephone service. If an IP Phone is reset, the IP Phone attempts to connect to the secondary system a number of times, defined by the S1 Retry Count of the IP Phone. Once its S1 Retry Count has expired, the IP Phone uses its S2 value to register directly to the primary system and receive service.

To ensure that Geographic Redundancy is available when required, the secondary system fault must be corrected and the system restored.

1+1 Planning

For a 1+1 configuration, plan the primary system as normal.

See *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120) and *Communication Server 1000E: Planning and Engineering* (553-3041-120) for details.

Planning the secondary system

Procedure 1 describes the high-level steps required to plan the secondary system.

When planning the secondary system:

- use the primary system as the starting point.
- determine the required redundant capacity and services from the primary system plan.
- identify the shelves, network groups, and circuit cards to install at the secondary site.

Procedure 1

Planning the secondary system

- 1 Copy the primary system plan.
- 2 Determine which services and capacity are required at the secondary site. Refer to the following sections for guidelines and recommendations:
 - “Common CS 1000E and CS 1000M Large System planning considerations” on page 46
 - “Planning considerations specific to CS 1000E” on page 49
 - “Planning considerations specific to CS 1000M Large System (CP PII)” on page 51
 - “Numbering plan” on page 54
 - “Branch Office support” on page 55

- 3 In the copied primary system plan, identify the circuit cards in the IPE shelves, network groups, or Media Gateway 1000Es (MG 1000Es) that are critical to provide the redundant features required from step 2.
- 4 Capture key details from the modified primary system plan in the secondary system plan.

End of Procedure

Common CS 1000E and CS 1000M Large System planning considerations

In the ideal 1+1 configuration, the secondary system is a duplicate of the primary system, with an identical number of MG 1000Es (for CS 1000E systems) or network groups and IPE shelves (for CS 1000M Large Systems) and the same circuit cards in the same slots. This duplication not only ensures that both systems operate identically, it also simplifies the planning, installation, and configuration of the secondary system.

However, installing the secondary system as a duplicate of the primary system is not always practical. For example, the secondary system cannot provide redundancy for traditional TDM line and analog line cards, so they are not required. Only those circuit cards that support the operation of IP Phones are necessary at the secondary site. This includes TDM equipment for providing digital media services to the IP Phones such as music and RAN.

In addition, if less capacity is required when the secondary system assumes system control, the secondary system can be configured with fewer shelves or MG 1000Es.

Missing hardware error messages

As the secondary system operates using a copy of the primary system database, it assumes that all of the same primary system hardware is available to it. Consequently, if any of the primary system's hardware is not installed at the secondary site, each endorsement of the replicated database will cause the secondary system to trigger alarms.

These error messages can be filtered or suppressed by the proper definitions of the Event Preference Table (EPT) in LD 117 on the secondary system. The

EPT is defined uniquely on the secondary system and is not replicated from the primary system database.

For more information on configuring the EPT, refer to *Software Input/Output: Maintenance* (553-3001-511).

Signaling Servers

The secondary CS 1000E or CS 1000M Large System, like the primary system, must have Signaling Servers installed to provide service to IP Phones. Signaling Servers at the secondary site must be configured independently from Signaling Servers at the primary site.

The number and configuration of Signaling Servers in the primary and secondary systems do not need to be the same. If traffic and capacity requirements are lower when the secondary system becomes active, fewer Signaling Servers can be installed at the secondary site. When this is the case, install enough Signaling Servers to handle the traffic created when the secondary system becomes active.

For more details on Signaling Server capacity, see *Communication Server 1000E: Planning and Engineering* (553-3041-120) and *Signaling Server: Installation and Configuration* (553-3001-212).

Route Data bBlock Node ID's

In a 1+1 Geographic Redundant configuration, the primary and secondary system both have the same identical customer database. The secondary system receives a copy of the primary system database whenever the primary system EDD's.

In the LD 15 Route data block (RDB) there is a prompt for Node ID for virtual trunks to reference the associated signaling server for that route. As the databases are the same, the node ID's will also be the same. This is design intent, but note it requires that the systems **MUST** be on 2 separate LAN subnets. This will normally not be an issue as the systems would typically be geographically separated and on separate LAN subnets. If a customer is setting the systems up side by side or for lab experimental purposes, they must keep in mind that they must be installed on separate subnets.

NRS

To support the IP Phone redirection process and to ensure that each system can properly route calls following a system failure, a Primary and Alternate Network Redirect Server (NRS) are required on the network. The Alternate NRS periodically synchronizes its database with the Primary NRS. This ensures that, if the Primary NRS fails, the Alternate NRS can assume the role of the Primary NRS.

To provide the necessary redundancy, each NRS must be installed in a different location. This can be accomplished by installing one NRS with each system or by installing each NRS in a remote location apart from either system. Wherever they are installed, ensure that at least one NRS remains operational following failure of either system.

For information on the required NRS routing entries for the 1+1 configuration, refer to “Numbering plan” on page 54. For additional information on installing and configuring the Primary and Alternate NRS refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

NCS

The Network Connect Server (NCS) is an application associated with the NRS that supports Geographic Redundancy. It allows the secondary system node TPS to query the NRS directly to perform the redirection of IP Phones to the primary system.

To support the 1+1 configuration, the NCS properties must be configured when the primary and secondary endpoints are defined on the NRS and when the primary and secondary system IP telephony nodes are defined in Element Manager (see *IP Peer Networking: Installation and Configuration* (553-3001-213) for details).

Vacant Number Routing

Vacant Number Routing (VNR) must be configured on the secondary system. If a DN is not valid, the number is considered vacant by the system call processor, and VNR is used to route the call to the NRS for resolution.

Time of day clock

The secondary system must always have the same time of day local clock as the primary system, regardless of the secondary site's actual time zone.

Network considerations

The primary and secondary systems must comply with network requirements as described in *Data Networking for Voice over IP* (553-3001-160). In addition, the primary and secondary systems must be installed in different LAN/WAN subnets. They must use the same NRS for routing.

Firewalls

The database-replication process requires FTP access to be allowed through the WAN between the primary and secondary systems. Therefore, the proper TCP/IP ports must be open on the appropriate security firewall servers.

Database-replication security

Given the importance and sensitivity of the database-replication transfer between the two systems, Nortel recommends installing Contivity (or similar security solution) between the ELAN FTP ports of the primary and secondary systems. This is recommended to ensure the security of the database transfer.

The following sections describe further considerations with respect to planning the secondary CS 1000E system and CS 1000M Large System, respectively.

Planning considerations specific to CS 1000E

For CS 1000E systems, plan the secondary site with the following component-specific considerations:

Call Server

The redundant dual Call Servers at the secondary site must be installed and configured identically to the primary system.

The software packages on the secondary system must provide the same functionality as those offered on the primary system. Any attempted

configuration differences on the secondary system will be overwritten during the database replication.

In addition, the GRPRIM package (404) must be equipped on the primary system and the GRSEC package (405) must be equipped on the secondary system.

Note: The GRSEC package (405) must be equipped during the software installation process; it cannot be added using a new keycode post software installation.

MG 1000E

To provide optimum performance, the MG 1000Es installed at both primary and secondary sites must be identical. That is, the same number of MG 1000Es must be equipped with the same circuit cards in the same slots.

A secondary system with fewer circuit cards or MG 1000Es is acceptable if partial redundancy is sufficient. However, installing fewer circuit cards or MG 1000Es will cause the system to output error messages identifying the missing hardware (see “Missing hardware error messages” on page 46).

The secondary system must also have service circuits providing music and RAN services.

When the following circuit cards are installed in MG 1000Es at the primary and secondary sites, they provide services when the secondary system assumes control:

- Media Cards
- Voice Gateway Media Cards
- Service Circuits used to provide services such as Music or Nortel Integrated Recorded Announcer
- CallPilot MGate cards (for use in Symposium voice processing applications)

The following circuit cards can be installed at the primary site, but they do not provide any services when the secondary system assumes control:

- Analog Line Cards

- Digital Line Cards
- Lineside T1 and E1 cards
- In-Skin Application Modules (such as Nortel Integrated Applications)
- Analog Trunk cards

MG 1000T

Given that the MG 1000T platform operates as an independent resource on the network, it is not encompassed by the Geographic Redundancy feature. However, if a failure is localized to the CS 1000E Call Servers and MG 1000Es, an MG 1000T located at the primary site can remain accessible when the secondary system assumes control.

This operational independence also means that the MG 1000T at the secondary site is always accessible from the primary system.

As an alternative, an MG 1000T can be installed at a remote third site separate from the primary or secondary systems. No matter where the MG 1000T is located, ensure that it has sufficient capacity to manage call volume if the primary system fails.

To increase overall system reliability, the MG 1000T can be configured as survivable.

For more information on MG 1000T capacity and survivability, see *Communication Server 1000E: Planning and Engineering* (553-3041-120).

Planning considerations specific to CS 1000M Large System (CP PII)

For a CS 1000M Large System (CP PII and CP PIV), plan the secondary system with the following component-specific considerations:

Call processors

The redundant dual call processors at the secondary site must be installed and configured identically to the primary system.

The software packages on the secondary system must provide the same functionality as those offered on the primary system. Any attempted configuration differences on the secondary system will be overwritten during the database replication.

In addition, the GRPRIM package (404) must be equipped on the primary system and the GRSEC package (405) must be equipped on the secondary system.

Note: The GRSEC package (405) must be equipped during the software installation process; it cannot be added using a new keycode post software installation.

Single-group

If the primary system is a CS 1000M SG system then the secondary system must be a CS 1000M SG as well.

Multi-group

If the primary system is a CS 1000M MG, then the secondary system can have fewer network groups. The secondary system must have a minimum of two CoreNet shelves (0 and 1) with clock controller, FIJI or IGS cards, and 2 IPE shelves. This allows the secondary system to retain the minimum multi-group infrastructure.

Core/Network modules

Nortel recommends that each Core/Network shelf have the following:

- cPCI CPU shelf with CP PII and CP PIV call processor, System Utility card, MMDU and cCNI card
- XCT cards providing conference ports
- XNET cards
- FIJI or IGS cards

IPE shelves

Each IPE shelf can be equipped with the following:

- Music XUT cards for music broadcast

- Integrated Recorded Announcer cards (if needed)
- Voice Gateway Media Cards providing transcoding between the TDM cards and IP portions of the equipment

While identical configuration of the primary and secondary systems is strongly recommended, installing fewer shelves and circuit cards at the secondary site is acceptable. However, this causes the system to output error messages identifying the missing hardware (see “Missing hardware error messages” on page 46 for further details).

Trunks

To install digital or analog trunks on the CS 1000M Large System, the trunk cards at each site must be installed in non-overlapping ranges: the common equipment card slots on the primary system that contain trunks (for example, PRI/PRI2 on DDP/DDP2 cards) must be left empty on the secondary system. The same rule is required for the trunk card slots on the secondary system: these card slots must be left empty on the primary system.

As a result, the presence of trunks causes a non-identical hardware configuration between the two systems. As the database must be configured to account for all equipment installed either on the primary system or the secondary system, error messages identifying the missing hardware are produced (see “Missing hardware error messages” on page 46 for further details).

To avoid this trunking limitation, the system can be configured with IP Peer Networking to provide the necessary trunking access from an MG 1000T or other peer node (see *IP Peer Networking: Installation and Configuration* (553-3001-213)).

Split network for CS 1000M Large Systems

If there are trunks (for example, PRI on DDP/DDP2 cards) equipped on the primary system, they are accessible when the primary system is operating in normal mode or when IP Phones registrations are split between the primary system and secondary system (for example, as a result of partial network connectivity problems). However, the PRIs become inoperable when the primary system is disabled.

Non-overlapping circuit card ranges

TDM circuit cards (for example, digital or analog line cards) can be installed at the secondary site that are not installed at the primary site, if the corresponding primary system slots are empty. To do so, configure the primary system database to take into account the extra secondary system equipment in addition to the primary system hardware.

If installing additional hardware at the secondary site, the primary system generates error messages as a result of the missing hardware. For more information, see “Missing hardware error messages” on page 46.

Numbering plan

As a result of the database replication process in the 1+1 configuration, the primary and secondary systems share the same HLOC definitions and IP Phone DNs. The NRS must therefore be configured to properly route IP Phone registrations to the primary system as well as route incoming Uniform Dialing Plan (UDP), Coordinated Dialing Plan (CDP), and VNR calls to the appropriate active system.

UDP calls and IP Phone registration redirection

In the 1+1 configuration, the HLOC value for the primary system endpoint must be configured on the NRS with the least-cost factor (that is, 1). This ensures that incoming UDP calls are directed to the primary system while it remains operational. This also allows IP Phone registration requests (that are routed using the HLOC value in the NUID) to be directed properly from the secondary system to the primary system. (See “Redirection process” on page 32 for details).

In addition, on the secondary system endpoint, the same HLOC value must be defined on the NRS, but with a higher cost factor (for example, 2). This allows the NRS to direct incoming UDP calls to the secondary system when the primary system fails.

Note: The NRS uses a polling mechanism to monitor the system status of both the primary and secondary systems. When the NRS detects a primary system failure, it can direct the incoming calls to the next available route: the secondary system.

CDP and VNR calls

To ensure that incoming CDP and VNR calls are routed appropriately, the range of IP Phone DNs used on both systems must be defined appropriately on the NRS for the two endpoints.

To ensure that incoming calls are directed appropriately to the primary system when it is active, the DN range must be configured on the primary system endpoint with the least-cost factor (that is, 1).

To ensure that the NRS directs the calls appropriately to the secondary system following primary system failure, the same DN range must be defined on the secondary endpoint with a higher cost factor (for example, 2).

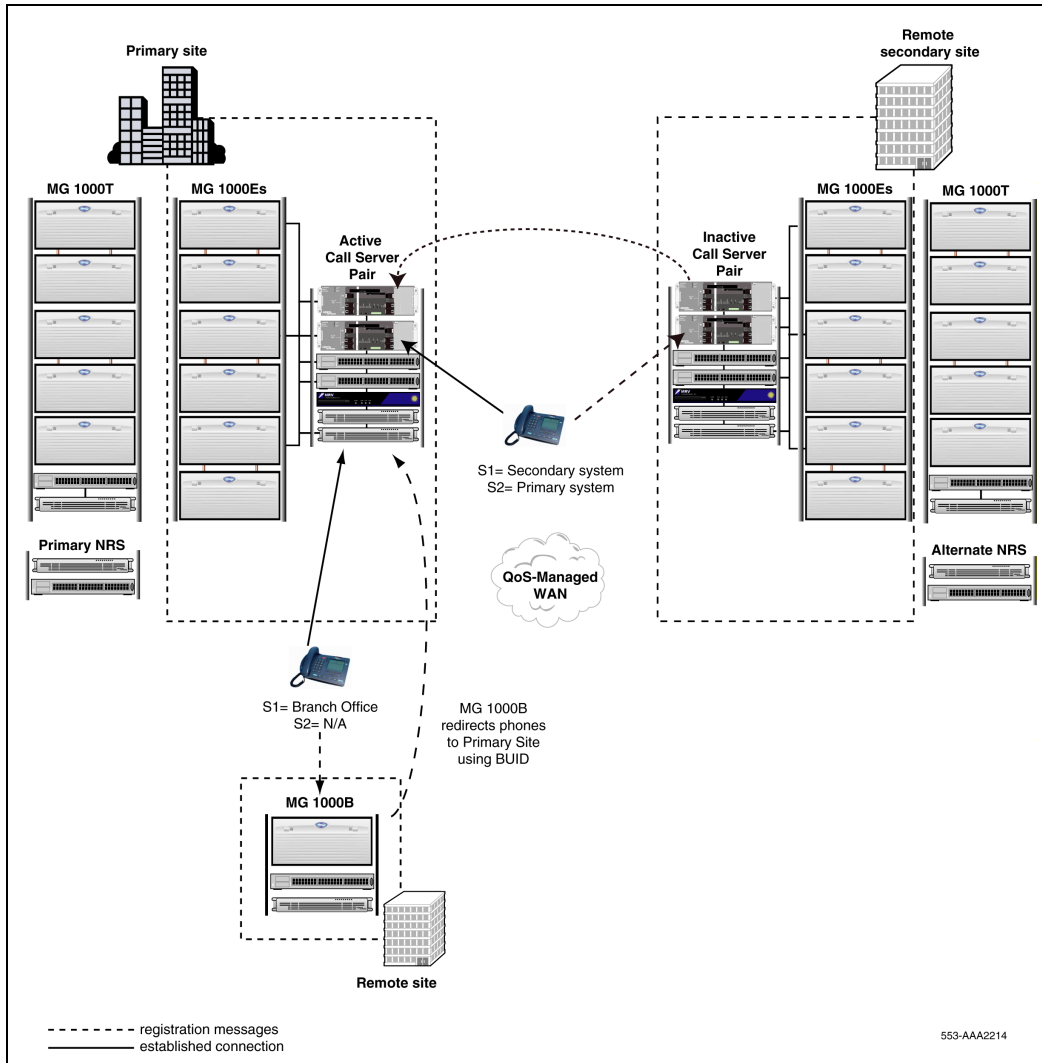
Branch Office support

The 1+1 configuration supports the Branch Office feature. To install a Media Gateway 1000B (MG 1000B), both the primary system and MG 1000B are configured according to the instructions in *Media Gateway 1000B: Installation and Configuration* (553-3001-214).

When the primary system is operational, it serves as the main office for the MG 1000B IP Phones. In case of failure of the primary system, the secondary system becomes the main office. The database-replication process ensures that the secondary system is configured appropriately when the primary system fails.

Figure 10 on [page 56](#) shows an MG 1000B installed in the 1+1 configuration.

Figure 10
1+1 configuration: Branch Office support



The MG 1000B can be configured as survivable in conjunction with Geographic Redundancy. In the unlikely event that both primary and

secondary systems fail, or, the WAN fails, the MG 1000B reverts to survivable.

NRS Routing for Branch Office

As the MG 1000B can operate with either the primary or secondary system functioning as the main office, the NRS must be configured to redirect MG 1000B IP Phones to the appropriate active system.

Note: To redirect IP Phones to the main office, the MG 1000B uses the Branch User ID (BUID) value of the IP Phone (configured in LD 11). The NRS routing entries required to support the redirection are dependent on the format of the BUID (either CDP- or UDP-based).

The NRS must also be configured to properly route incoming UDP, CDP, and VNR calls to the MG 1000B IP Phones, when these are registered to the primary system, to the secondary system, or to the MG 1000B at the branch office.

UDP

When the MG 1000B IP Phones are registered on the primary or secondary system, the NRS definitions required to properly route incoming UDP calls to these IP Phones are the same as those required for standard IP Phones in the 1+1 configuration, as described in “UDP calls and IP Phone registration redirection” on page 54. Specifically, on the NRS, the HLOC for the primary system endpoint must be defined with the least-cost factor (that is, 1) and the same HLOC value must be defined for the secondary system endpoint with a higher cost factor greater than 100 (for example, 102). Incoming UDP calls are then routed to the appropriate active home system.

In the unlikely event that both the primary and secondary systems fail, an additional NRS definition is required to ensure survivability of the MG 1000B. The branch office HLOC must be defined on the branch office endpoint with the least-cost factor. This additional entry ensures that UDP calls can reach the MG 1000B when the primary and secondary systems are both unavailable.

Note: Since the HLOC value at the branch office is different than the HLOC value of the primary and secondary systems, the UDP dial-in number to the MG 1000B IP Phones is different when both home office systems fail.

BUID redirections with UDP

If the BUIDs are based on the UDP dialing plan (that is, BUID = AC (AC1/AC2 of branch office)+ HLOC (of GR system) + DN), the HLOC routing entry on the NRS used to route incoming calls also supports the registration redirection requests for the MG 1000B. When the MG 1000B queries the NRS with the BUID to determine the home system of the IP Phone, the NRS responds with the active home system: primary or secondary.

CDP and VNR

When the MG 1000B IP Phones are registered on the primary or secondary system, the NRS definitions required to route incoming CDP calls to these IP Phones are similar to those required for standard IP Phones in the 1+1 configuration, as described in “CDP and VNR calls” on page 55. Specifically, the range of main office DNs used for the MG 1000B IP Phones must be configured on the NRS as least-cost for the primary system and higher-cost for the secondary system. This ensures that incoming CDP calls to the MG 1000B IP Phones are routed to the active home system.

These CDP entries also support the VNR call rerouting coming from the MG 1000B.

In the unlikely event that both the primary and secondary systems fail, a third NRS definition is required to ensure survivability of the MG 1000B. The same DN range must be defined on the branch office endpoint with a higher cost factor than the primary and secondary system endpoints. This entry ensures that CDP calls are rerouted to the MG 1000B when the primary and secondary systems are both unavailable.

BUID redirections with CDP

If the BUIDs are based on the CDP dialing plan (that is, BUID = DN), the CDP routing entry on the NRS used to route incoming calls also supports registration redirection requests for the MG 1000B. When the MG 1000B

queries the NRS with the BUID to determine the home system of the IP Phone, the NRS responds with the active home system: primary or secondary.

1+1 configuration NRS routing example

Table 3 provides sample numbering plan values used in a 1+1 configuration that is supporting an MG 1000B using the Branch Office feature.

Table 3
Sample values for 1+1 configuration

Variable	Value
Primary system ID	0_gr
Secondary system ID	1_gr
Main Office IP Phone DN ranges	2200-2299
Primary system HLOC (secondary system HLOC is the same)	344
Branch office ID	BO
Branch office HLOC	347
MG 1000B IP Phone DN range	2400-2499
SRG50 ID	SRG
SRG50 Office HLOC	349
SRG50 IP Phone DN Range	2500-2599

In this example, the DN prefix 22 is used for on-net CDP routing and VNR for the primary and secondary system IP Phones. For the MG 1000B IP Phones, the DN prefix 24 is used. For the SRG50 IP phones the DN prefix is 25.

For incoming UDP calls to the primary and secondary system and for the redirection of IP Phones to their appropriate home system, the HLOC 344 is used. For incoming UDP calls to the branch office when the primary and

secondary system fail, the HLOC 347 is used. For incoming UDP calls to the SRG50 when the primary and secondary system fail, the HLOC 349 is used.

In the general, the route cost for the home gateway endpoint (S1 in the IP phone) must be greater than 100. This stipulation is in place to accommodate redirection of IP phones.

Table 4 on page 60 shows the NRS configurations for this example.

Table 4
Routing across various scenarios

System	DN Prefix	DN Type	Route Cost	SIP URI Phone Context
Primary	344	Level1 regional	1	geo_udp
Primary	22	Level0 regional	1	geo_cdp.geo_udp
Primary	24	Level0 regional	1	geo_cdp.geo_udp
Primary	25	Level0 regional	1	geo_cdp.geo_udp
Secondary	22	Level0 regional	102	geo_cdp
Secondary	24	Level0 regional	2	geo_cdp
Secondary	25	Level0 regional	2	geo_cdp
Secondary	344	Level0 regional	101	geo_udp
Secondary	34424	Level0 regional	2	geo_udp
Secondary	34425	Level0 regional	2	geo_udp
Standby	343	Level1 regional	101	geo_udp
Main office	8	Level0 regional	1	geo_cdp.geo_udp
Branch / SRG	8	Level0 regional	101	geo_cdp.geo_udp
Standby	8	Level0 regional	2	geo_cdp.geo_udp

Installing a 1+1 configuration

To perform the Geographic Redundancy 1+1 installation and configuration, follow the steps in Procedure 2.

Procedure 2 **Installing 1+1 configuration**

- 1** Install the primary system.
 - a.** Install hardware (if required).
 - b.** Install CS 1000 Release 4.0 software, including GRPRIM package.
 - c.** Install the customer database (if required).

Note: For more detailed instructions on installing a system, see *Communication Server 1000E: Installation and Configuration* (553-3041-210) or *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210):

- 2** Configure the primary system for 1+1 (see “Configuring the primary system” on page 64):
 - a.** Configure Backup Rules in LD 117.
 - b.** Configure the Geographic Redundancy Data Base Replication Control Block in LD 117.
 - c.** Configure Geographic Redundancy State Control Block in LD 117.

- 3 Install secondary system:
 - a. Install hardware in accordance with the secondary system plan (see “Planning the secondary system” on page 45).
 - b. Install software, including GRSEC package.

Note: The GRSEC package (405) must be equipped during the software installation process; it cannot be added using a new keycode post software installation.

Note: Ensure that the Problem Determination Tool (PDT) access password is the same on the secondary system as it is on the primary system; otherwise, the database replication process will fail.
 - c. Set up the secondary system specific customer database (very limited data required):
 - i. Configure Ethernet Protocol in LD 117.
 - ii. Configure Point-to-Point protocol in LD 117, if needed.
 - iii. Configure Event Preference Table (EPT).
- 4 Install and configure the Signaling Servers
- 5 Install the Primary and Alternate NRS and configure IP Peer Networking (see *IP Peer Networking: Installation and Configuration* (553-3001-213)).
- 6 Configure VNR on the secondary system.
- 7 On the primary system, perform a data dump (EDD) in LD 43 to invoke the Automatic Backup to the secondary system.
- 8 On the secondary system, perform the following:
 - a. Log out from the system and wait until SRPT4643 is displayed. This message notifies that a new backup data file has arrived. Otherwise, after the manual restore and sysload, another automatic restore can occur (if ARSTR is defined YES) followed by an automatic sysload (if SYSLD is defined YES).
 - b. Define backup rule number 1 on the secondary system for restoring the first database received from the primary system (see “Configure Backup Rule in LD 117” on page 64).

- c. Define GRDRC Block with
Rule for BKUP = 1
Rule for Restore = 1
ARSTR = NO
ASYSLD = NO

See “Configure Database Replication Control Block for Geographic Redundancy in LD 117” on page 68.

- d. Initiate a manual restore from the backup data received from the primary system by entering the following command in LD 43:

RSR 1

Where 1 is the Restore Rule defined in the GRDRC block in step c (otherwise, all system-specific definitions are lost).

- e. Perform a manual sysload to endorse the backup database.
- 9** Install (if required) and configure the IP Phones with S1 pointing to the secondary system node TPS and S2 pointing to the primary system node TPS. See *Communication Server 1000E: Installation and Configuration* (553-3041-210) for instructions on installing IP Phones.

End of Procedure

Configuring the primary system

The following configurations must be performed on the primary system:

- “Configure Backup Rule in LD 117” on page 64.
Note: It is necessary to define only one backup rule that is used for both backup on the primary system and restore on the secondary system.
- “Configure Database Replication Control Block for Geographic Redundancy in LD 117” on page 68.
- “Configure Geographic Redundancy State Control Block in LD 117” on page 71.

Note: When these configurations are made at the primary system, the applicable definitions are only implemented at the secondary system when the database replication process is completed successfully.

Configure Backup Rule in LD 117

To perform the database-replication process, a Backup Rule must be defined on the primary system. The Backup Rule identifies the destination ELAN network interface IP address on the secondary system for the database replication. It also defines the number of versions of the database that are kept on the secondary system.

To complete the database replication successfully, the Backup Rule must be referenced in the Database Replication Control Block. See “Configure Database Replication Control Block for Geographic Redundancy in LD 117” on page 68 for details.

The secondary system also uses the Backup Rule during the database-restore operation to identify the appropriate database to restore. Configure the Backup Rule in LD 117 as follows:

LD 117 – Configure Backup Rule

Command	Description
NEW BKPR xxx aaa b...b yy	<p>Add a new Backup Rule, where:</p> <ul style="list-style-type: none"> xxx = Backup Rule number ID = 1-100. aaa = rule type = SCS. Currently, this is the only rule type that exists; it allows direct replication to another system. b...b = ELAN network interface IP address of the destination system. yy = the number of database versions to save on the destination system = (2)-10.
CHG BKPR xxx aaa b...b yy	<p>Change a Backup Rule, where:</p> <ul style="list-style-type: none"> xxx = Backup Rule number ID = 1-100. aaa = rule type = SCS. Currently, this is the only rule type that exists; it allows direct replication to another system. b...b = ELAN network interface IP address of the destination system. yy = the number of database versions to save on the destination system = (2)-10.
OUT BKPR xxx	<p>Remove backup rule, where:</p> <ul style="list-style-type: none"> xxx = Backup Rule number ID = 1-100
PRT BKPR xxx	<p>Print backup rule, where:</p> <ul style="list-style-type: none"> xxx = Backup Rule number ID = 1-100 <p>If no rule number is entered, then all Backup Rules are printed.</p>

Note: A backup rule can also be defined on the secondary system to provide replication to the primary system after a long-term failure. For details, refer to “Primary system recovery” on page 77.

Configure Backup Rule in Element Manager

To configure a Backup Rule in Element Manager, follow the steps in Procedure 3.

Procedure 3

Configuring Backup Rule in Element Manager

- 1 To add or edit a Backup Rule in Element Manager, in the Element Manager navigator, click **Services > Backup and Restore > Call Server > Rules**.

The **Backup Rules** web page appears. See Figure 11.

Figure 11
Backup Rules page

Rule	Type	Name	IP address	User Name	Versions kept	Edit	Delete	Backup History
1	FTP	ftp rule	47.11.228.94	plarivie	2	Edit	Delete	Backup History
2	SCS	scs rule	47.11.228.81		5	Edit	Delete	Backup History

- 2 To add a Backup Rule, click the **to Add** button.
(To edit a Backup Rule, click the **Edit** button next to the rule to be edited.)
The **Backup Rule Configuration** web page appears. See Figure 12 on [page 67](#).

Figure 12
Backup Rule Configuration page

Input Description	Input Value
Rule Number:	1
Rule Type:	FTP (FTP)
Rule Name:	ftp rule
IP Address of FTP server:	47.11.228.94
Login Name:	plamie
Password:	
Password Confirmation:	
Path:	cs1000/backups
Number of versions kept:	2

Submit Refresh Delete Cancel

Not for Confidential Information

3 Configure the Backup Rule as follows:

- In the **IP address** text box, enter the ELAN network interface IP address of the destination system for the database replication
- In the **Number of versions kept** text box, enter the number of database versions to save on the destination system.

4 Click **Submit**.

Note: The **Rule Number** text box is automatically populated with the lowest available rule number.

End of Procedure

Configure Database Replication Control Block for Geographic Redundancy in LD 117

To perform the database-replication process, the Geographic Redundancy Database Replication Control (GRDRC) Block must be configured on the primary system. The GRDRC Block defines how the database replication is initiated on the primary system and whether the secondary system restore and sysload operations are performed automatically or manually.

Note: Only one GRDRC block can be created on the system. If the GRDRC block is not defined on the primary system, the Geographic Redundancy database replication is not activated.

Configure the GRDRC Block in LD 117 as follows:

LD 117 – Configure GRDRC Block. (Part 1 of 2)

Command	Description
NEW GRDRC xxx aaa yyy bbb ccc	<p>Add a GRDRC block, where:</p> <ul style="list-style-type: none"> • xxx = Backup Rule number. • aaa = how the automatic database replication to the destination system occurs: <ul style="list-style-type: none"> — (IMM) - immediately after any data dump operation — MIDN - after midnight data dump only — NO - not allowed • yyy = Restore Rule = Backup Rule number used for the restore operation. • bbb = (YES)/NO. Defines whether or not the automatic restore operation is allowed. • ccc = (YES)/NO. Defines whether or not the automatic sysload after successful automatic restore is allowed. ccc = YES is only allowed if bbb = YES.

LD 117 – Configure GRDRC Block. (Part 2 of 2)

Command	Description
CHG GRDRC xxx aaa yyy bbb ccc	<p>Change current GRDRC block, where:</p> <ul style="list-style-type: none"> • xxx = Backup Rule number. • aaa = how the automatic database replication to the secondary system occurs: <ul style="list-style-type: none"> — (IMM) - immediately after any data dump operation — MIDN - after midnight data dump only — NO - not allowed • yyy = Restore Rule = Backup Rule number used for the restore operation. • bbb = (YES)/NO. Defines whether or not the automatic restore operation is allowed. • ccc = (YES)/NO. Defines whether or not the automatic sysload after successful automatic restore is allowed. ccc = YES is only allowed if bbb = YES.
OUT GRDRC	Remove current GRDRC Block.
PRT GRDRC	Print GRDRC Block.

For information on performing manual backup and restore operations, see “Manual database replication and restore” on page 81.

Configure Database Replication Control Block for Geographic Redundancy in Element Manager

To configure the Database Replication Control Block in Element Manager, follow the steps in Procedure 4 on [page 70](#).

Procedure 4

Configuring Database Replication Control Block in Element Manager

- 1 In the Element Manager navigator, click **System > Geographic Redundancy > Database Replication Control**.

The **Database Replication Control** web page opens. See Figure 13.

Figure 13
Database Replication Control page

The screenshot shows the 'Database Replication Control' page in the Nortel CS 1000 Element Manager. The page has a purple header with the Nortel logo and 'CS 1000 ELEMENT MANAGER'. On the left is a navigation tree with categories like Home, Links, System, IP Telephony, Customers, Routes and Trunks, Dialing and Numbering Plans, and Services. The main content area is titled 'Database Replication Control' and contains a table with two columns: 'Input Description' and 'Input Value'.

Input Description	Input Value
Backup Rule Number for Backup (BKUP_RULE):	1
Automatic Replication backup (ABKUP):	After each data dump (IMM)
Backup Rule Number for Restore (RSTR_RULE):	1
Automatic Replication restore (ARSTR):	<input checked="" type="checkbox"/>
Automatic Sysload (ASYSLD):	<input checked="" type="checkbox"/>

At the bottom of the form are four buttons: Submit, Refresh, Delete, and Cancel.

- 2 Enter the desired **Backup Rule Number for Backup (BKUP_RULE)**.
- 3 Choose the **Automatic Replication backup (ABKUP)** value from the drop-down list.
- 4 Enter the **Backup Rule Number for Restore (RSTR_RULE)**.
- 5 To allow the automatic restore operation, click the **Automatic Replication restore (ARSTR)** check box.
- 6 To allow the automatic sysload operation, click the **Automatic Sysload (ASYSLD)** check box.

7 Click **Submit**.

End of Procedure

Configure Geographic Redundancy State Control Block in LD 117

The GRSC Block specifies the secondary system state control parameters that allow the system to transition from INACTIVE to ACTIVE states (for more information, see “Secondary system operating states” on page 39).

Only one GRSC Block can be created in the system. If the GRSC Block is not defined, the default values are used.

Configure the GRSC Block in LD 117 as follows:

LD 117 – Configure GRSC Block.

Command	Description
NEW GRSC xxx yyy zzz a..a	<p>Add a new GRSC block, where:</p> <ul style="list-style-type: none"> xxx = the number (N) of IP Phones that must register on the secondary system for the system to escalate to the ACTIVATING state. If no value is entered, xxx = 1. The maximum value of xxx is: 10% x (Basic IP User License + IP User License). yyy = Short Term Failure Timer, in minutes = (5) - 600 zzz = Failure Clearance Timer, in minutes = (5) - 180 a..a = Secondary system Deactivation Mode = (AUTO)/MAN
CHG GRSC xxx yyy zzz a..a	<ul style="list-style-type: none"> Change current GRSC block, where: xxx = the number (N) of IP Phones that must register on the secondary system for the system to escalate to the ACTIVATING state. If no value is entered, xxx = 1. The maximum value of xxx is: 10% x (Basic IP User License + IP User License). yyy = Short Term Failure Timer, in minutes = (5) - 600 zzz = Failure Clearance Timer, in minutes = (5) - 180 a..a = Secondary system Deactivation Mode = (AUTO)/MAN
OUT GRSC	Remove GRSC Block.
PRT GRSC	Print GRSC Block.

Note 1: If SDAM = MAN is defined, the deactivation process on the secondary system can be initiated only by entering the CLR GR command in LD 135. (See “Secondary system ACTIVE operation” on page 75 for details).

Note 2: Nortel recommends defining SDAM = MAN during a long-term maintenance window on the primary system (for example, when moving the primary system to a new location).

Configure Geographic Redundancy State Control Block in Element Manager

To configure the Geographic Redundancy State Control block using Element Manager, follow the steps in Procedure 5.

Procedure 5

Configuring Geographic Redundancy State Control Block in Element Manager

- 1 From the Element Manager navigation tree, choose **System > Geographic Redundancy > State Control**.

The **State Control** web page opens. See Figure 14 on [page 74](#).

Figure 14
State Control page

NORTEL CS 1000 ELEMENT MANAGER Help | Logout

Managing: **Buffy 1 (47.11.140.8)**
System > Geographic Redundancy > State Control

State Control

Input Description	Input Value
Geographic Redundancy Threshold (GRTHR):	<input type="text" value="1"/>
Short Term Failure Timeout in minutes (STFTO):	<input type="text" value="5"/>
Fault Clearance Timeout in minutes (FCTO):	<input type="text" value="5"/>
Secondary CS Deactivation Mode (SDAM):	<input type="text" value="Automatic (AUTO)"/>

http://47.11.140.12/fs/nav/navtree.htm#H_352_2_35_3

- 2 Enter the desired values for the **Geographic Redundancy Threshold (GRTHR)**, **Short Term Failure Timeout in minutes (STFTO)**, and **Fault Clearance Timeout in minutes (FCTO)** in the appropriate text boxes.
- 3 Select the **Secondary CS Deactivation Mode (SDAM)** from the drop-down list.
- 4 Click **Submit**.

————— **End of Procedure** —————

Configuring primary (S1) and secondary (S2) Connect Servers

To install and configure IP Phones, refer to *Communication Server 1000E: Installation and Configuration* (553-3041-210). Ensure the S1 of each IP Phone points to the secondary system node TPS, and the S2 points to the primary system node TPS.

To configure IP Phones using DHCP, refer to *Data Networking for Voice over IP* (553-3001-160).

Secondary system ACTIVE operation

When the secondary system is in the ACTIVE state following primary system failure, administrative changes made on the secondary system can be preserved.

Before making any changes, define ARSTR = NO in the GRDRC block (see “Configure Database Replication Control Block for Geographic Redundancy in LD 117” on page 68). This prevents the automatic restore process from accidentally overwriting the latest changes made on the secondary system.

The secondary system administrative changes can then be saved by performing a data dump.

Clear ACTIVE state

If the secondary system is in the ACTIVE state and the secondary system Deactivation Mode is defined as Manual (SDAM = MAN) in the GRSC block, clear the secondary system ACTIVE state in LD 135 by entering the following on the secondary system:

LD 135 – Clear Geographic Redundancy

Command	Description
CLR GR	Clear secondary system ACTIVE state. This command triggers repetitive attempts to redirect all the IP Phones to the primary system for a maximum period defined by FCT. If the primary system is operational, N falls below GRTHR, and the system transitions to the DEACTIVATING state.

Clear ACTIVE state in Element Manager

To clear the secondary system ACTIVE state in Element Manager, follow the steps in Procedure 6.

Procedure 6

Clearing secondary system ACTIVE state in Element Manager

- 1 In the Element Manager navigator, choose **System Status > Call Server > Core Common Equipment Diagnostics**.

The **Core Common Equipment Diagnostics** web page opens. See Figure 15 on [page 77](#).

Figure 15
Core Common Equipment Diagnostics page

Site: 47.11.254.121 > System Status > Call Server >

Core Common Equipment Diagnostics

Diagnostic Commands	Command Parameters	Action
STAT CPU - Core status for both CPUs	(none)	Submit
ENL CNI - Enable CNI card/port(c=side,s=slot,p=port)	(c# s#/c# s# p#)	Submit
TEST CPU - Test the inactive core	(none)	Submit
SCPU - Switch cores	(none)	Submit
STAT HEALTH HELP - Help for health commands	(none)	Submit
STAT GR - Status of Geographic Redundancy	(none)	Submit
STAT GR - Status of Geographic Redundancy		
TEST GR - Test Geographic Redundancy		
CLR GR - Clear operation for the secondary CS		

Instruction: Select command, add value and click on [Submit]

- 2 From the **Diagnostic Commands** drop-down lists, choose **CLR GR - Clear operation for the secondary CS**.
- 3 Click **Submit**.

End of Procedure

Primary system recovery

When the primary system experiences a long-term failure, any administrative changes made on the active secondary system during this period are saved on the secondary system only. These changes can be preserved and replicated to the primary system once it returns to normal operations.

Procedure 7 describes how to perform a system recovery following primary system failure.

Procedure 7
Recovering the primary system database

- 1 On the secondary system:
 - a. Define a new Backup Rule in LD 117 using the IP address of the primary system (see “Configure Backup Rule in LD 117” on page 64 for details).
 - b. Perform a data dump in LD 43.
(As the secondary system is equipped with the GRSEC package, this does not automatically initiate a backup to the primary system).
 - c. Still in LD 43, enter:

BKR <BKUP rule>

Where <BKUP rule> is the Backup Rule defined in 1a.

This manually initiates the database replication to the primary system (see “Manual database replication and restore” on page 81 for more details).

- 2 On the primary system:
 - a. In LD 43, enter the following:

RSR <RULE for Restore> 1

Where <Rule for Restore> must be the Restore Rule defined in the GRDRC block on the primary system (otherwise, all system-specific definitions are lost).

This manually restores the database that was just transferred to the primary system.

- b. Perform a sysload to endorse the newly restored data.

End of Procedure

Procedure 8 describes how to perform a system test following primary system recovery.

Procedure 8**Testing the recovered primary system**

1 On the primary system:

a. In LD 117, enter the following:

CHG GRDRC <BKUP rule> IMM <Rule for Restore> YES YES

where <BKUP rule> and <Rule for Restore> are both the original Backup Rule for replication to the secondary system (not the rule defined in Procedure 7).

b. Perform a data dump in LD 43.

The data dump will initiate the automatic database replication to the secondary system.

2 On the secondary system:

a. Enter LD 117, and define ARSTR = YES and ASYSLD = YES in the GRDRC data.

b. Log off the system and wait for the automatic restore and automatic sysload to take place to endorse the backup database.

End of Procedure

Upgrades

If a system upgrade or patch is required, both the primary and secondary systems must be upgraded to have the matching software issue. The upgrades must be performed separately at the primary and secondary sites.

More importantly, for the database-replication process to function normally during the upgrades, upgrade the secondary system before the primary system. This allows the secondary system to perform an automatic conversion of older database versions that arrive while the primary system is temporarily running the older software.

Note: If the primary system attempts to transfer a database version that is higher than the secondary system software, the automatic restore is blocked and a warning message is printed on the TTY.

The primary and secondary systems conform to existing methodologies to deploy maintenance and diagnostic patches as implemented in CS 1000 Release 4.0 software.

Maintenance

The Primary and Secondary systems conform to the methods and procedures used for local and remote access as defined for CS 1000M Large Systems and CS 1000E systems.

Geographic Redundancy implementation preserves all existing VxWorks or overlay support tools available on the CS 1000M Large System or CS 1000E solutions except where enhancements are noted in this NTP.

OTM 2.2

OTM 2.2 can be used to administer the primary and secondary systems in a 1+1 configuration. The primary and secondary systems are represented in OTM as separate systems. System-specific changes made on one system (such as IP addresses and EPT definitions) do not affect the other system. The secondary system view can be created in OTM by cloning the primary system data and then updating the system-specific information for the secondary system.

Database configuration

During normal operation, the primary system is the master of the customer database. Perform all database modifications on the primary system only, by direct administration or through OTM.

Manual database replication and restore

To manually invoke the database replication and restore in LD 43, refer to the following:

LD 43 – Manually invoke database replication and restore operations

Command	Description
BKR xx	Invoke database-replication operation, where: <ul style="list-style-type: none">xx = Backup Rule number. This command is typically entered on the primary system for replication to the secondary system.
RSR xx yy	Restore the database, where: <ul style="list-style-type: none">xx = Restore Rule number on the local system. This value must be the same as the Restore Rule defined in the local system's GRDRC block; otherwise, all system-specific definitions are lost.yy = database version number. If no version number is entered, the most recent backup (1) will be used. The latest database version is assigned the highest priority. For example: yy = 1 restores the latest backup database; yy = 2 restores the second latest database version. This command is typically entered on the secondary system to restore a database received from the primary system.

Manual database replication in Element Manager

To manually invoke the database replication process in Element Manager, follow the steps in Procedure 9.

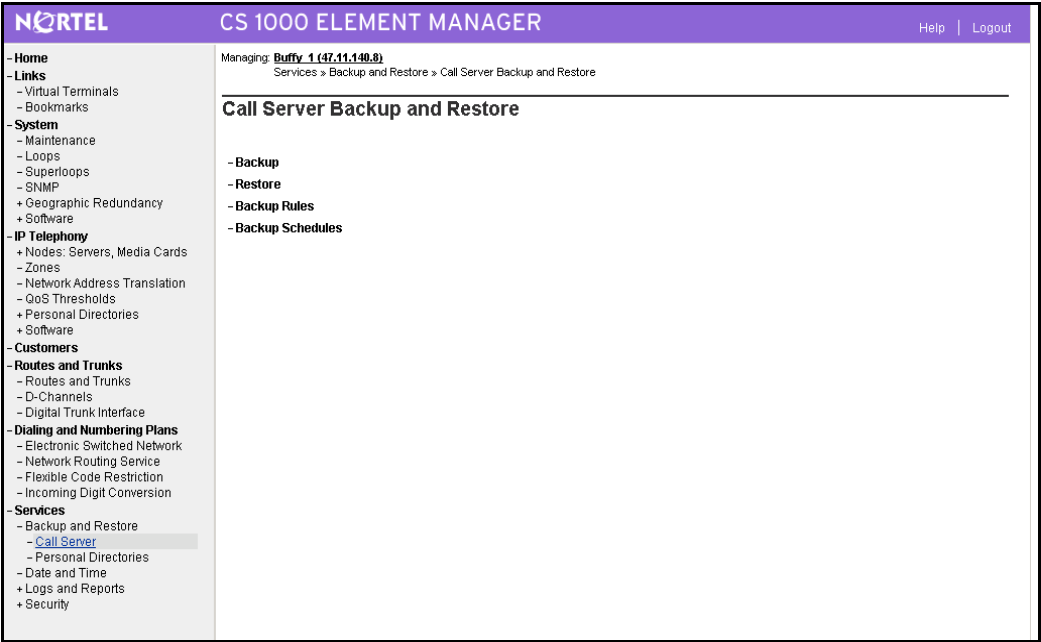
Note: This command is typically entered on the primary system for replication to the secondary system.

Procedure 9 Manually invoking the database replication in Element Manager

- 1
- In the Element Manager navigator, click **Services > Backup and Restore > Call Server**.

The **Call Server Backup and Restore** web page opens. See Figure 16.

Figure 16
Call Server Backup page



- 2
- Click **Backup**.

The **Call Server Backup** web page opens. See Figure 17 on [page 83](#).

Figure 17
Call Server Backup page

The screenshot displays the 'Call Server Backup' page in the CS 1000 ELEMENT MANAGER. The left sidebar contains a navigation menu with the following items: Home, Links (Virtual Terminals, Bookmarks), System (Maintenance, Loops, Superloops, SNMP, Geographic Redundancy, Software), IP Telephony (Nodes: Servers, Media Cards, Zones, Network Address Translation, QoS Thresholds, Personal Directories, Software), Customers, Routes and Trunks (Routes and Trunks, D-Channels, Digital Trunk Interface), Dialing and Numbering Plans (Electronic Switched Network, Network Routing Service, Flexible Code Restriction, Incoming Digit Conversion), and Services (Backup and Restore, Call Server, Personal Directories, Date and Time, Logs and Reports, Security). The main content area is titled 'Call Server Backup' and shows the 'Action' drop-down menu with the following options: Backup, Backup Clear(EDD CLR), and Backup According to Rule(BKR X). The 'Backup' option is selected. The 'Submit' and 'Cancel' buttons are visible next to the drop-down menu.

- 3 From the **Action** drop-down list, select **Backup According to Rule (BKR X)**.

The **Backup Rule Number** drop-down list appears.

- 4 From the **Backup Rule Number** drop-down list, select the desired rule number.
- 5 Click **Submit**.

End of Procedure

Manual database restore in Element Manager

To manually invoke a database restore process in Element Manager, follow the steps in Procedure 10.

Note: This command is typically entered on the secondary system to restore a database received from the primary system.

Procedure 10

Manually invoking the database restore in Element Manager

- 1 In the Element Manager navigator, click **Services > Backup and Restore > Call Server**.

The **Call Server Backup and Restore** web page opens. See Figure 16 on [page 82](#)).

- 2 Click **Restore**.

The **Call Server Restore** web page opens. See Figure 18 on [page 85](#).

Figure 18
Call Server Restore page

NORTEL CS 1000 ELEMENT MANAGER Help | Logout

Managing: **Buffy 1 (47.11.140.8)**
 Services > Backup and Restore > Call Server Backup and Restore > Call Server Restore

Call Server Restore

Action Restore from Backup Data(RES) Submit Cancel

- Restore from Backup Data(RES)
- Database issue and creation date(DAT)
- Restore According to Rule(RSR X'Y)
- Backup data versions(DAT R V)

- From the **Action** drop-down list, select **Restore According to Rule (RSRXY)**.

The **Backup Rule Number** and **Restore Version** drop-down lists appear.

- In the **Backup Rule Number** drop-down list, enter the Backup Rule number to use for the restore operation.

Note: The system uses the specified Backup Rule to identify the appropriate database to restore.

- In the **Restore Version** drop-down list, enter the appropriate version of the backup file to restore (typically the latest: 1).
- Click **Submit**.

End of Procedure

1+1 Geographic Redundancy testing

Secondary system operation can be tested from the primary system using LD 135. The Test command gracefully drops the registration of the specified IP Phone, so that it registers with the secondary system. This test ensures that the secondary system operates properly when the primary system fails.

Note: “Network connectivity failure - call scenarios” on page 93 provides a description of sample call scenarios that are applicable during these tests.

Initiate the Geographic Redundancy tests on the primary system in LD 135 as follows:

LD 135 – 1+1 configuration test

Command	Description
TEST GR I s c u	<p>Activate test for the IP Phone specified by TN, I s c u</p> <p>This command simulates primary system failure by dropping the registration of the IP Phone on the primary system.</p> <ul style="list-style-type: none"> Registration for an idle IP Phone is dropped immediately. Registration for a busy IP phone is dropped when the IP phone becomes idle. The IP Phone must then be reset to trigger registration to the secondary system. Once the IP Phone registers on the secondary system, it displays “Local Mode” or “Local Mode: Invalid ID”. Only one IP Phone can be tested at one time. If a selective test is already running on another IP Phone, this command switches the test to the new specified IP Phone.
TEST GR CLR	<p>Clear selective test. The IP Phone is allowed to re-register to the primary system.</p> <p>Once this command is issued, the affected IP Phone must be reset to drop the secondary system registration and re-register to the primary system.</p>

1+1 Geographic Redundancy testing in Element Manager

To perform 1+1 Geographic Redundancy testing in Element Manager, follow the steps in Procedure 11.

Procedure 11

Performing 1+1 Geographic Redundancy testing in Element Manager

- 1 From the Element Manager navigation tree, choose **System Status > Call Server > Core Common Equipment Diagnostics**. The **Core Common Equipment Diagnostics** web page appears (see Figure 15 on [page 77](#)).
- 2 From the **Diagnostic Commands** drop-down lists, choose **Test GR - Test Geographic Redundancy** and enter the appropriate terminal number (TN), in l s c u format, for the IP Phone to be tested.
- 3 Click **Submit**.

Note: The IP Phone must now be reset to trigger registration to the secondary system.

End of Procedure

IP Phone Test Local Mode

Although the IP Phone Test Local Mode is typically used to register an IP Phone to the local MG 1000B, it can also be used to test Geographic Redundancy. In this case, instead of reverting to the MG 1000B SSC, Test Local Mode switches the IP Phone registration from the primary system to the secondary system (or from the home system to the backup system in the Controlled Load-Sharing configuration). Call scenarios can then be performed to ensure that the IP Phone is functional when it is registered at the secondary system.

Note: For Test Local Mode to function properly, the tested IP Phone must be registered to the primary (or home) system and have S1 addressing the secondary (or backup) system.

Procedure 12 on [page 88](#) describes how to perform the Test Local Mode operation on an IP Phone.

Procedure 12
Performing Test Local Mode

- 1 Press the **Services** key to bring up the Options menu as shown in Figure 19.

Figure 19
Options menu

Options
Telephone Option
Virtual Office Login
Test Local Mode
Select

- 2 Use the Down key to highlight **Test Local Mode**.
The IP Phone displays “Local Mode”.
- 3 Perform call scenarios to ensure that the IP Phone is still functional.
- 4 To re-register to the primary site, scroll down to select the **Resume Normal Mode** command.

Note: If the user forgets to return to Normal Mode, the secondary (or backup) system redirects the IP Phone to the primary (or home) system after a period of ten minutes.

End of Procedure

Full system test

In order to perform a full system test, the administrator must mimic a full primary system failure. This can be accomplished by, for example, powering down the primary system, disconnecting the primary Call Server ELAN network interface cables, or by disabling the ELAN network interface on the primary system by using the DIS ELNK command in LD 137. This triggers the IP Phones to register to the secondary system, allowing test call scenarios to be performed.

1+1 system status

The status of each system in the 1+1 configuration can be obtained in LD 135. On the primary system, the system status identifies when the last successful database replication was completed, as well as whether the replication process is operating properly.

On the secondary system, the system status identifies the secondary system operating state, as well as the time and date of the last successful restore and sysload operations.

Obtain a system status for the primary or secondary system in LD 135 as follows:

LD 135 – 1+1 configuration status.

Command	Description
STAT GR	Print current status of 1+1 Geographic Redundancy on the specified system.

Figure 20 shows a sample output of the STAT GR command on the primary Call Server.

Figure 20
1+1 Geographic Redundancy Status on primary system

```
Geographic Redundancy Status
-----

Primary Call Server
Automatic Replication Backup defined: NO / IMM / MIDN1
Last Successful Replication Backup2
mode: Manual / Automatic
Backup Rule number: 100
performed at: hh:mm on MM DD, YYYY
(Failed Backup attempts: x, last one at: hh:mm on MM DD, YYYY)3
Test activated: None / Selective for IP set l s c u
Internet phones registered locally: x
```

Note 1: Printed only if GRDRC is configured.

Note 2: Printed only if GRDRC is configured.

Note 3: Printed only if the last backup attempt failed.

Figure 21 shows the sample output of the STAT GR command on the secondary system:

Figure 21
1+1 Geographic Redundancy Status on secondary system

```
Geographic Redundancy Status
-----
Secondary Call Server
Automatic Replication Restore defined: NO / YES
Automatic Sysload defined: NO / YES
Last Backup arrived from Primary CS at hh:mm on MM DD, YYYY
Last Successful Replication Restore
mode: Manual / Automatic
Backup Rule number: 100
performed at: hh.mm on MM DD, YYYY
of backup data received at: hh.mm on MM DD, YYYY
Last Sysload for restored data endorsement
Successful / Failed
performed at: hh:mm on MM DD, YYYY
Internet phones registered locally: x
Geographic Redundancy status: Secondary CS Inactive/
Activating/
Calmdown/
Active/
Deactivating/
Outoflicense
(Days remaining in licensed period x)1
(Licensed period is exceeded)2
```

Note 1: This line is printed only if the secondary Call Server is in the ACTIVE state.

Note 2: This line is printed only if the secondary Call Server is in the OUTOFLICENSE state.

Note 3: Lines displaying information about database replication are printed only if GRDRC block is defined.

1+1 system status in Element Manager

To obtain the 1+1 system status in Element Manager, follow the steps in Procedure 13.

Procedure 13

Obtaining 1+1 system status in Element Manager

- 1 From the Element Manager navigation tree, choose **System Status > Call Server > Core Common Equipment Diagnostics**.

The **Core Common Equipment Diagnostics** web page appears (see Figure 15 on [page 77](#)).

- 2 From the **Diagnostic Commands** drop-down lists, choose **Stat GR - Status of Geographic Redundancy**.
- 3 Click **Submit**.

End of Procedure

System faults

FTP transfer failure

During an automatic backup attempt, if the primary system fails to gain FTP access to the secondary system, it attempts to gain access again for a total of five attempts, with a delay of 40 seconds between attempts.

Note: This scenario allows the primary system to overcome short term inoperability of the secondary system of about 200 seconds (for example, for initialization).

In case of backup attempt failure, the following appears when the primary system status is printed (using the STAT GR command in LD 135):

```
Failed Backup attempts: x, last one at: hh:mm on MM DD,
YYYY
```

Once the FTP transfer to the secondary system is performed successfully, the counter is cleared and the Failed Backup attempts information no longer appears in the primary system status.

Secondary system database endorsement failure:

On the secondary system, each database replication sysload produces the following message:

```
SRPT4645: The system will automatically be restarted
for Data Endorsement
```

If an automatic data endorsement sysload fails due to technical difficulty on the secondary system, the following automatic actions are performed:

- 1 The system reverts to the last database files that were successfully loaded prior to the last restore.
- 2 One more sysload is activated with a new reason notified by:

```
SYS0139 Database Replication Endorsement failed
```

Network connectivity failure - call scenarios

This section describes call processing scenarios that apply in the event of network connectivity failure in the 1+1 configuration. This particular case describes a situation where, due to connectivity problems, some IP Phones can connect to the primary system while others cannot. The IP Phones that cannot access the primary system are still able to access the secondary system.

This results in a registration split: some IP Phones are registered at the primary system, while others are registered at the secondary system.

In this case, the following call processing scenarios apply.

Call processing scenario 1

An IP Phone (or other telephone) that is on the local system calls another locally registered IP Phone.

Result

Local call is established.

Call processing scenario 2

A locally registered IP Phone dials an external number.

Result

Call is established (as long as the given system maintains connectivity with the NRS).

Call processing scenario 3

An incoming external call comes to the DN of an IP Phone registered on a system.

Result

The connection is established.

Call processing scenario 4

An incoming external call comes to a DN on the secondary system for an IP Phone that is currently registered on the primary system.

Result

Vacant Number Routing mechanism is activated to resolve the call.

Call processing scenario 5

An IP Phone that is now registered on the secondary system dials a local number for an IP Phone that remains registered on the primary system.

Result

Vacant Number Routing is activated and resolves the call.

Call processing scenario 6

An IP Phone (or other telephone) that is on the primary system dials a local number for an IP Phone that is now registered on the secondary system.

Result

The primary system cannot resolve the call.

Note: This is similar to the main office in a Branch Office configuration: VNR can only reroute calls for vacant DN's that have an associated NUID.

Feature interactions

CDR

CDR reports are accumulated separately on the primary system and secondary system and are consolidated when processed.

CallPilot

The following steps are required to provide redundancy for CallPilot:

- On the primary CallPilot system, perform periodic (nightly) system backups to a network drive.
- Arrange for the data on the network drive to be mirrored to the secondary site (using a customer-provided mechanism).
- When a switchover occurs, retrieve the latest backup and restore it on the secondary CallPilot.
- Reconfigure the secondary CallPilot with settings matching the system to which it is connected.

Symposium

The following steps are required to provide redundancy for Symposium:

- Periodically back up Primary Symposium Call Center Server (SCCS) onto the Secondary SCCS
- When switchover occurs, perform the following:

- Change Standby Host Name (including reboot)
- Computer Name Sync (including reboot)
- Change Standby TLAN IP address
- Run Server Setup Configuration (including reboot)
- Start SCCS Services
- Change Keycode

System monitoring

Given the importance of the secondary system for operation of the 1+1 configuration, Nortel recommends implementing Simple Network Management Protocol (SNMP) alarm management to monitor the health of the system. SNMP can be used to trigger alarms, for example, when the secondary system state changes and when any IP Phone unregisters from the primary system. SNMP can also be implemented to monitor the health of the systems.

For more information, see *Simple Network Management Protocol* (553-3001-519).

Limitations

When the primary system fails, established active calls between IP Phones (where the conversation stage speech path goes through direct set-to-set Real-time Transport Protocol [RTP]) are not dropped for a limited time (watchdog timer). During this time, no call modification is available. When the call is completed (release key is pressed on one of the telephones), the IP Phones are reset.

Idle IP Phones stay registered with the primary TPS for ten minutes. At the end of ten minutes, the IP Phones reset and register to the secondary system TPS. If the Release key is pressed on an IP Phone within ten minutes, it resets immediately.

Geographic Redundancy Controlled Load-sharing configuration

Contents

This section contains information on the following topics:

Description	98
Normal operation	99
Site 1 system failure	103
Site 2 system failure	105
Planning a Controlled Load-sharing configuration	106
Numbering plan	110
Branch Office support	112
Installing a Controlled Load-sharing configuration	116
Maintenance	117
Feature interactions	118
System monitoring	118

Description

The Controlled Load-sharing configuration increases the reliability of CS 1000M Large Systems (CP PII and CP PIV) and CS 1000E systems through configuration of two geographically-separated systems that provide redundancy for each other. In this configuration, both systems are active and perform call processing for their local telephones. In case of failure of either system, the remaining active system can assume control of the failed system's IP Phones and provide service as normal.

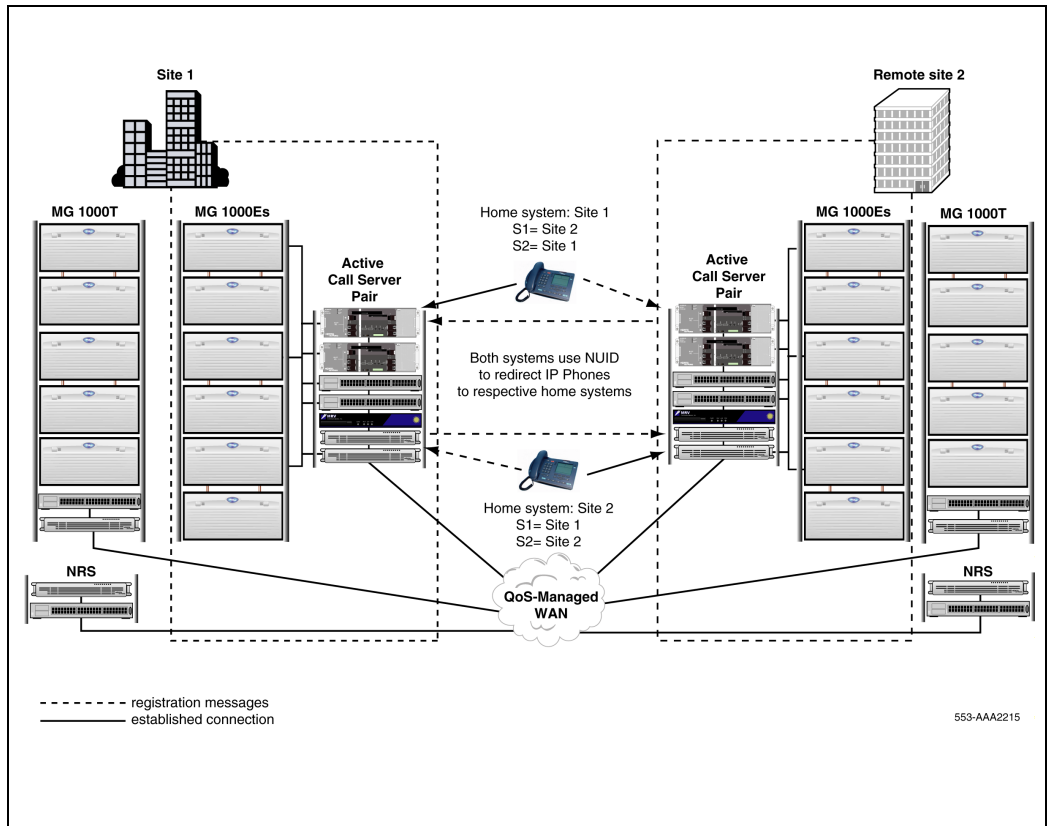
The two systems in a Controlled Load-sharing configuration do not have to be of the same type. CS 1000M Large Systems and CS 1000E systems can be backed up by either a CS 1000M Large System or CS 1000E system.

Note: The Controlled Load-sharing configuration provides redundancy for IP Phones only. Redundancy for analog (500/2500-type) telephones and digital telephones is not supported. Analog (500/2500-type) and digital telephones can still be connected to a system, but they will not be operational if that system fails.

Normal operation

Figure 22 shows two CS 1000E systems in a Controlled Load-Sharing configuration.

Figure 22
Controlled Load-Sharing configuration



Connectivity between the two systems is provided through a QoS-managed WAN.

Note: As the MG 1000T platform operates as an independent network resource, it is not encompassed by the Controlled Load-sharing configuration. You can collocate the MG 1000T with each system for convenience. However, provided the MG 1000T is operational, it remains available to both systems at all times.

The Controlled Load-sharing configuration employs similar functionality to the Branch Office feature. For each IP Phone, a DN and TN must be configured on a home system, where the IP Phone ultimately registers. At the backup system, the IP Phone is also assigned a DN and TN. This ensures that the backup system can provide the necessary functionality in case of failure at the home system.

Note: The DNs and TNs configured on the home and backup systems must be duplicates.

On the backup system, each IP Phone is also manually assigned a Network User ID (NUID) and Network Home TN (NHTN), similar to the Branch User ID (BUID) and Main Office TN (MOTN). The NHTN corresponds to a home system TN; the NUID corresponds to a dialable home system DN where the IP Phone ultimately registers. As a result, the backup system can use the NUID value in order to redirect IP Phones to the home system for registration.

Redirection process

In the Controlled Load-sharing configuration, each redundant IP Phone's primary Connect Server (S1) points to its backup system. When the IP Phone powers up, it registers first with the backup system node Terminal Proxy Server (TPS), then with the backup system itself. The backup system, reading the IP Phone's NUID, automatically redirects the IP Phone to the home system — the backup TPS queries the NRS for the IP address of the home system node indicated by the NUID. When it receives a positive response, the IP Phone is redirected to the home system.

IP Phones remain registered at the backup system only if the connection to the home system is lost.

While each IP Phone's S1 points to its backup system, its secondary Connect Server (S2) must point to its home system. This ensures that the IP Phones

can register directly to their home system and continue normal operations if the connection to their backup system is lost.

In Figure 22 on [page 99](#), both systems serve at once as home and backup systems: each system provides service to IP Phones that are registered locally and redirects IP Phones to their home systems. As a result, the two systems back each other up.

Database configuration

Unlike the 1+1 configuration, the Controlled Load-sharing configuration provides no database replication. The databases must therefore be configured manually at each site.

The Controlled Load-sharing configuration provides additional flexibility in the possible hardware and software configurations at either site as the systems are not constrained by the necessity to duplicate hardware and software. Instead, systems are only limited by the need to provide the required redundant capacity and services for the additional IP Phones.

In order to simplify database administration, the TN range used for the redundant IP Phones must be the same on the home and backup systems. As well, configure the IP Phones with the same DN, TN, and features at both sites for feature and application consistency.

As the CS 1000E systems and CS 1000M Large Systems use the same TN mapping format (l s c u), there is no conflict when a backup system is of a different type than the home system.

In addition, there are no limitations on installing IP Phones, analog (500/2500-type) telephones, or digital telephones that have no redundancy requirements on either system.

Software

To implement the Controlled Load-sharing configuration, there are no additional software packages required on either system. The software packages required for the 1+1 configuration, 404 (GRPRIM) and 405 (GRSEC), do not apply to the Controlled Load-sharing configuration.

However, the two systems must run CS 1000 Release 4.5 (or later) software. Software installation, including installation of patches, is performed separately for each system.

Ideally, the software packages on the backup system must provide the same functionality as those offered on the home system. However, this is not a necessity if less functionality is acceptable at the backup system. Regardless, ensure that the backup system has sufficient capacity and User Licenses available to provide redundancy for the additional IP Phones.

Hardware

With the Controlled Load-sharing configuration, there is greater flexibility available in configuring the hardware at both sites. The only physical constraint on a backup system is to have sufficient hardware to provide the capacity and the appropriate range of matching TNs required to service the additional redundant IP Phones.

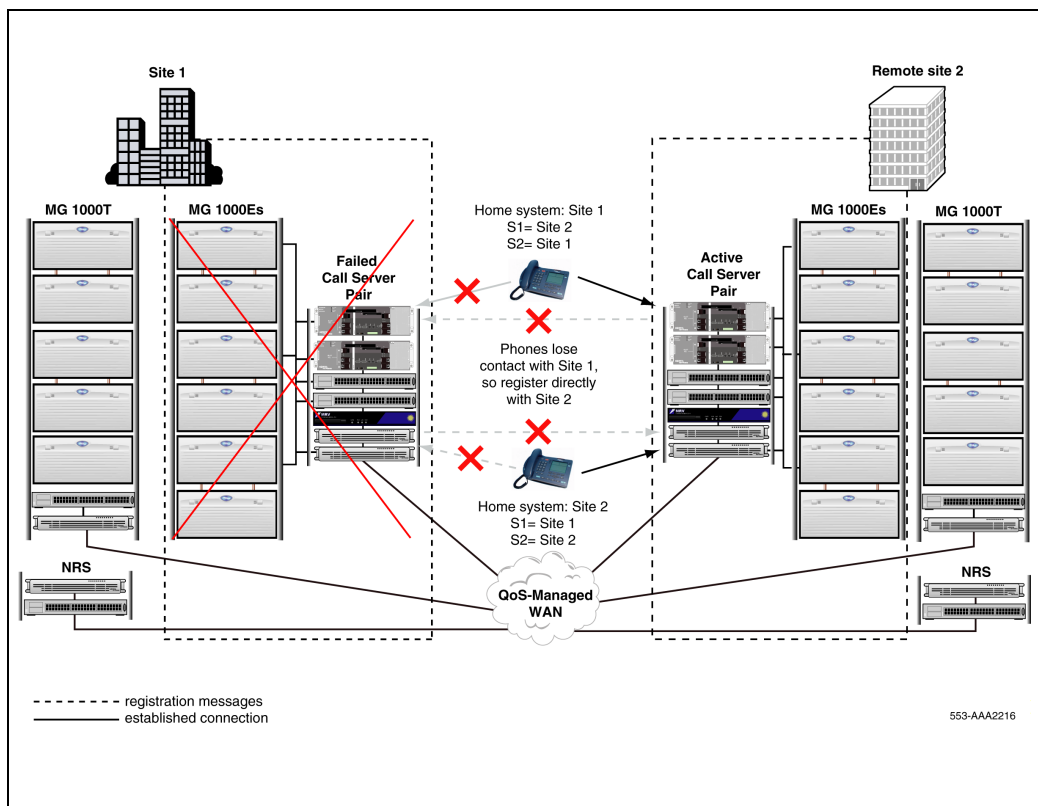
The backup system can be configured to provide the same basic features and services as the home system. This is not a requirement if fewer services on the backup system is acceptable.

Carefully plan the backup system to provide the necessary redundant capacity required. For further planning details, see “Planning a Controlled Load-sharing configuration” on page 106.

Site 1 system failure

Figure 23 shows a Controlled Load-sharing configuration that is experiencing a failure at Site 1.

Figure 23
Load-sharing configuration: system failure at Site 1



If the IP Phones in the network cannot connect to Site 1 because of a system failure (or network connectivity problem), the IP Phones act as follows:

- **Site 1 = Home system:** If Site 1 is their home system (S2), the IP Phones stay registered with the Site 1 TPS for ten minutes. At the end of ten minutes, the IP Phones reboot and register first to the backup system TPS at Site 2, as normal (if the Release key is pressed on an IP Phone within ten minutes, it resets immediately)

Note: Active calls between IP Phones are maintained for a limited time, but no call modification is available and, when the call is completed, the IP Phones are restarted.

The backup system then attempts to once again redirect the IP Phones to Site 1. When the redirection attempt fails, the IP Phones remain registered at Site 2, where they then obtain normal service. While they remain registered at Site 2, the IP Phones display “Local Mode”.

Once connectivity to Site 1 is restored, the IP Phones are automatically redirected again to their home system.

Note: Established calls are completed before the redirection to the home system.

- **Site 1 = Backup system:** If Site 1 is their backup system (S1), the IP Phones registered at Site 2 continue to receive normal telephone service. If an IP Phone is reset, it attempts to connect to Site 1 a number of times, defined by the S1 Retry Count of the IP Phone. Once the S1 Retry Count of the IP Phone has expired, the IP Phone then uses its S2 value to register directly to Site 2.

Note: Unlike the 1+1 configuration, the Controlled Load-sharing configuration does not offer a transition of states on the backup system.

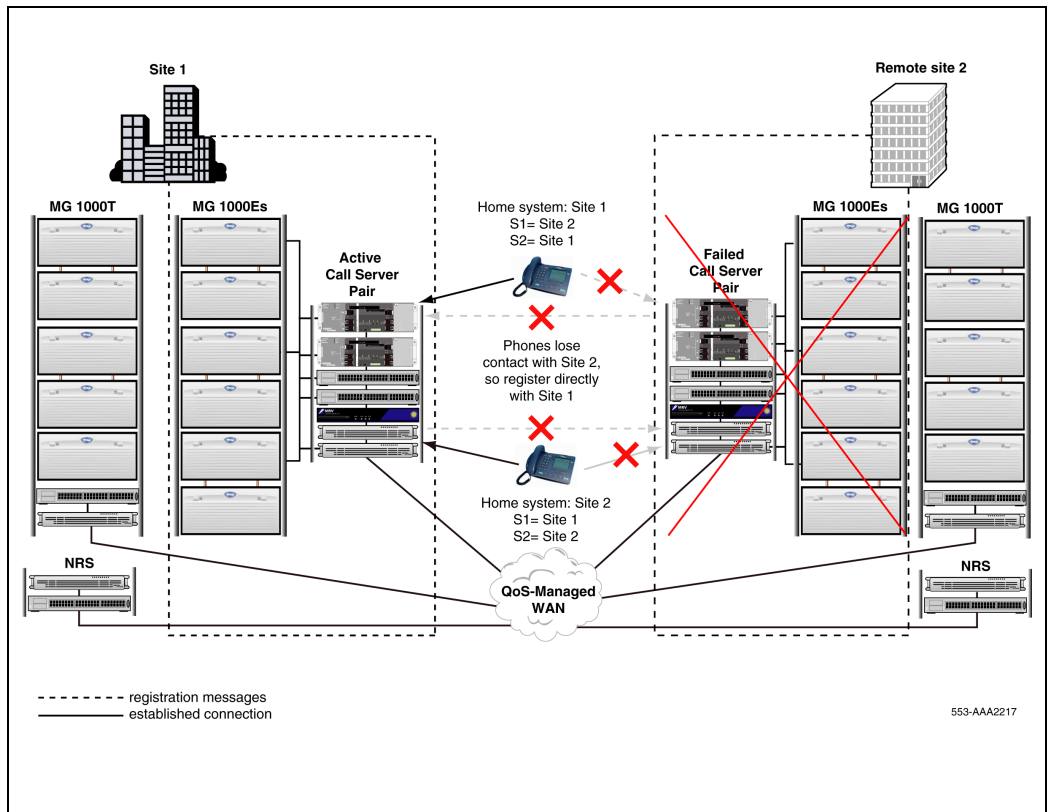
When the IP Phones are registered on Site 2, users have full access to the features and services configured on that system.

Site 2 system failure

Site 2 system failure operates in a similar manner to Site 1 system failure, with the exception that Site 1 assumes control of the IP Phones.

Figure 23 shows a Controlled Load-sharing configuration that is experiencing a failure at Site 2.

Figure 24
Controlled Load-sharing configuration: system failure at Site 2



Planning a Controlled Load-sharing configuration

Planning the systems in a Controlled Load-sharing configuration is different from a 1+1 configuration as neither system is constrained by the configuration of the other system.

To implement the Controlled Load-sharing configuration, plan each system to service all of the home and backup telephones that are to be defined on that system. That is, plan the system as though all telephones, including local telephones and redundant IP Phones that are going to be redirected to the opposite site, are registered at the local site. This ensures that the required capacity and services are available to provide redundancy in case the opposite site fails.

The home and backup systems must share the 3-digit NODE ID prefix, and redundant IP Phones defined with the same TNs and DN's on the home and backup systems.

Finally, each system can be planned independently to provide different features and services. If one system is configured with less hardware or fewer features and services, ensure that it is acceptable for the affected IP Phones to have less redundant capacity.

Additional planning considerations

The Controlled Load-sharing configuration provides redundancy only for IP Phones. Therefore, only those circuit cards that support the operation of IP Phones can be configured for redundancy. This includes TDM equipment for providing digital media services to the IP Phones, such as music and Integrated Recorded Announcer.

Each system can be configured to provide local service to analog (500/2500-type) and digital telephones. However, these telephones are inoperable when the local system fails.

Signaling Servers

Both home and backup CS 1000E systems or CS 1000M Large Systems must have Signaling Servers installed in order to provide service to IP Phones. The Signaling Servers at each site must be configured independently.

Signaling Server requirements are site-specific and can vary in number and configuration at each site. If one site has lower traffic and capacity requirements, it can have fewer Signaling Servers installed, provided they can handle the traffic created when the other system fails.

For more details on Signaling Server capacity, see *Communication Server 1000E: Planning and Engineering* (553-3041-120) and *Signaling Server: Installation and Configuration* (553-3001-212).

Enhanced Redundancy for IP Line nodes

To allow IP Phones to register to the different nodes at the home and backup sites, the Controlled Load-sharing configuration uses the Enhanced Redundancy for IP Line nodes feature. This feature relaxes the checking performed by a node on the Node ID that is presented by a registering IP Phone. It allows an IP Phone with a three-digit Node ID to register to a node that is configured with a four-digit Node ID. To enable the registration, the three-digit Node ID of the IP Phone must match the first three digits of the node's four-digit Node ID. For more information, see *IP Line: Description, Installation, and Operation* (553-3001-365).

For example, if the home system node number is 1110, then the backup system must use the same leading three digits, 111, in its node number (for example, 1115). The IP Phones must then be configured with the same three digits, 111, when defining its Node information. The IP Phone can then connect successfully to both Node ID 1110 and 1115. In fact, it can connect successfully to any Signaling Server that has 111 as the prefix of its node number.

NRS

To support the IP Phone redirection process and to ensure that each system can properly route calls following a system failure, a Primary and Alternate Network Redirect Server (NRS) are required on the network. The Alternate NRS periodically synchronizes its database with the Primary NRS. This ensures that, if the Primary NRS fails, the Alternate NRS can assume the role of the Primary NRS.

To provide the necessary redundancy, each NRS must be installed in a different location. This can be accomplished by installing one NRS with each system or by installing the NRSs in different remote locations. Wherever they

are installed, you must ensure that at least one NRS remains operational following failure of either system.

For information on the required NRS routing entries for the Controlled Load-sharing configuration, refer to “Numbering plan” on page 110. For additional information on installing and configuring the Primary and Alternate NRS refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

NCS

The Network Connect Server (NCS) is an application associated with the NRS that supports Geographic Redundancy. It allows the backup system node TPS to query the NRS directly to perform the redirection of IP Phones to the home system.

To support the Controlled Load-sharing configuration, the NCS properties must be configured when the home and backup endpoints are defined on the NRS and when the home and backup system IP telephony nodes are defined in Element Manager (see *IP Peer Networking: Installation and Configuration* (553-3001-213) for details).

Vacant Number Routing

Vacant Number Routing (VNR) must be configured on each backup system. If a DN is not valid, the number is considered vacant by the system call processor, and VNR is used to route the call to the NRS for resolution.

Time of day clock

The date and time display on each IP Phone is determined by the system to which the IP Phone connects. In the case of system failure, the idle clock on the IP Phone display must be localized to the correct time for the geographic location of the IP Phone.

Because the systems in a Controlled Load-sharing configuration can be located in regions with different time zones, the configuration supports the Branch Office feature that enables a different time zone to be specified for telephones at multiple sites. Each site must have the appropriate time zone configured for the IP Phones at the other site. In the case of system failure,

the time zone adjusts the system time for display at the appropriate site. Idle IP Phones then display the correct time for their area.

For more information, see Appendix B: “Controlled Load-sharing zones” on [page 175](#).

User Licenses

In the Controlled Load-sharing configuration, User Licenses are required for all IP Phones that a system is backing up in addition to the telephones that are registered locally on the system.

Data network planning

The home and backup systems must comply with network requirements as described in *Data Networking for Voice over IP* (553-3001-160). The home and backup systems use a common NRS for routing.

MG 1000T

The MG 1000T platform operates as an independent resource on the network; therefore, it is not encompassed by the Controlled Load-sharing feature. However, if a site’s cause of failure is localized to the CS 1000E Call Servers and MG 1000Es, an MG 1000T located at the same site can remain accessible when the system control transfers from a home system to a backup system.

NUID

The Network user ID (NUID) for each IP Phone must match the IP Phone’s dialable DN at the home system.

If the NUID is not configured, the IP Phone registers directly on the backup system. If the IP Phone is configured with a NUID and Network Home TN, the IP Phone is automatically redirected to the home system TPS and then to the home office system.

An NUID has a maximum of 15 digits. Under the Uniform Dialing Plan (UDP), the NUID consists of the Access Code (AC1/AC2 of backup system), the Home Location (HLOC of home system), the Location Code (LOC) and the home system DN, (for example, 6 343-5555). Under the Coordinated Dialing Plan (CDP), it can be an extension (for example, 4567).

Note: The home system DN must be an Electronic Switched Network (ESN)-compliant DN.

To create the NUID, use one of the following DN keys defined at the IP Phone's home system TN: ACD, MCN, MCR, PVN, PVR, SCN or SCR.

Note: If ACD (Automatic Call Distribution) key is used to create the NUID, the ACD DN or Message Center DN must be used.

For more information about CDP and UDP dialing plans, refer to *Dialing Plans: Description* (553-3001-183).

Network Bandwidth Management

The Network Bandwidth Management feature allows bandwidth zones to be configured on a network basis. This enables codec selection and bandwidth allocation software to identify whether IP Phones or Media Gateways are physically collocated (in the same bandwidth zone) even though they are controlled by different Call Servers.

Numbering plan

The Controlled Load-sharing configuration is designed to work only if the two systems use a common dialing plan. Any other configuration is not guaranteed to work properly.

As well, the DNs and TNs configured on both systems for the redundant IP Phones must match.

The NRS must be configured to properly route IP Phone registrations to the home system. It must also be configured to route incoming UDP, CDP, and VNR calls to the appropriate active system.

UDP calls and IP Phone registration redirection

In the Controlled Load-sharing configuration, the HLOC value for the home system endpoint must be configured on the NRS with the least-cost factor (that is, 1). This ensures that incoming UDP calls are directed to the home system while it remains operational.

In addition, the separate HLOC value for the backup system endpoint must be defined on the NRS, also with the least-cost factor. This allows the NRS to direct incoming UDP calls to the backup system when the home system fails.

Note 1: When the home system fails, the UDP dial-in numbers for redundant IP Phones will be different (as a result of the different HLOC values of the backup and home systems).

Note 2: The NRS uses a polling mechanism to monitor the system status of both the home and backup systems.

NUID redirections with UDP

If the NUIDs are based on the UDP dialing plan (that is, $NUID = AC + HLOC + DN$), the HLOC routing entry on the NRS used to route incoming calls to the home system also supports the registration redirection requests to the home system. When the backup system TPS queries the NRS with the NUID to determine the home system of the IP Phone, the NRS responds with the least-cost route: the home system.

CDP and VNR calls

To ensure that incoming CDP and VNR calls are routed appropriately, the matching range of redundant IP Phone DNs used on both systems must be defined appropriately on the NRS for the two endpoints.

To ensure that incoming calls are directed appropriately to the home system when it is active, the DN range must be configured on the home system endpoint with the least-cost factor (that is, 1).

To ensure that the NRS directs the calls appropriately to the backup system following home system failure, the same DN range must be defined on the backup endpoint with a higher cost factor (for example, 2).

NUID redirections with CDP

If the NUIDs are based on the CDP dialing plan (that is, $NUID = DN$), the CDP routing entry on the NRS used to route incoming calls also supports registration redirection requests to the home system. When the backup system queries the NRS with the NUID to determine the home system of the IP Phone, the NRS responds with the least-cost route: the home system.

Branch Office support

The Controlled Load-sharing configuration supports the Branch Office feature only when CDP BUID form is used. Then two levels of redundancy can be received and appropriate NRS definitions are:

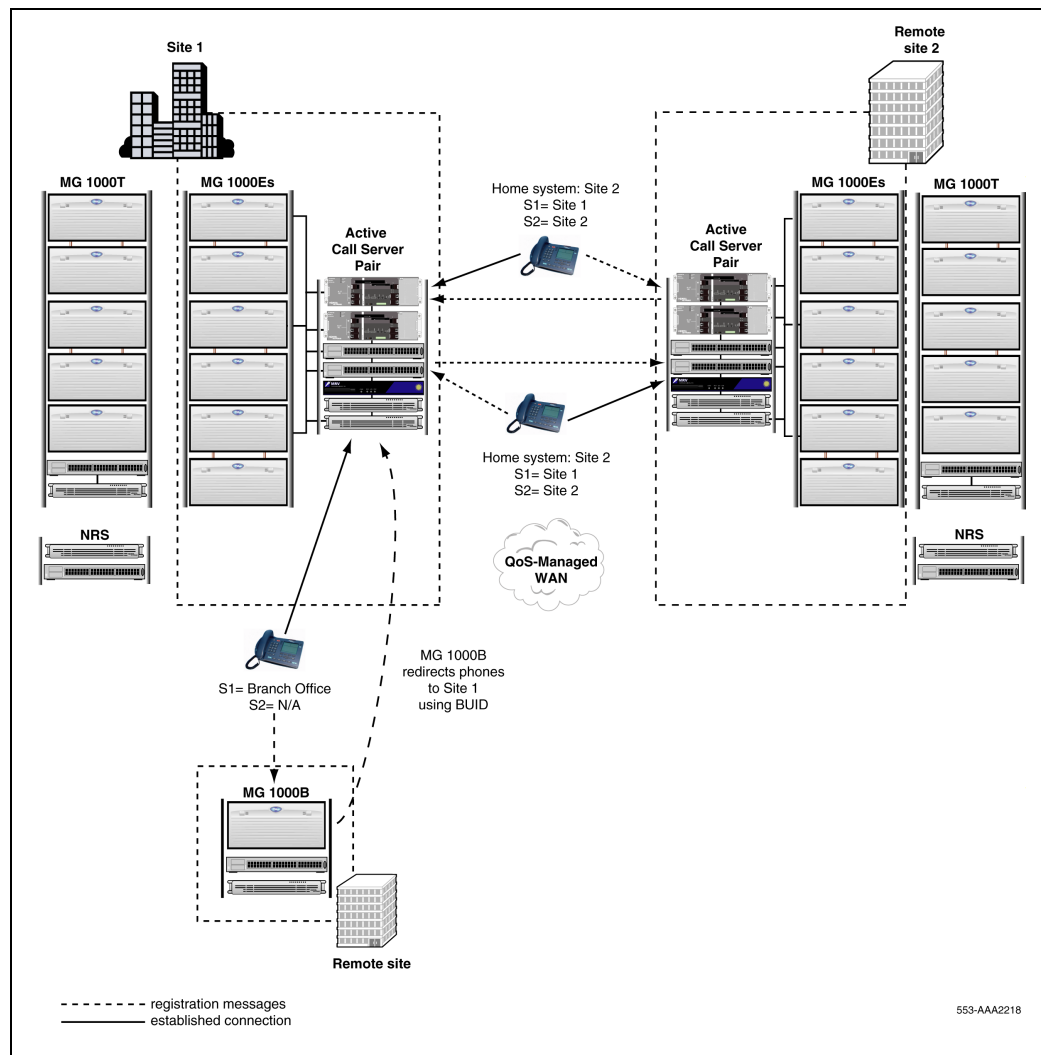
- for home system home-corresponding CDP entry is defined with cost factor 1
- for backup system - cost factor 2
- for branch office - cost factor 3

Otherwise, if the BUID UDP form is chosen, then one level of redundancy can be received; only one of the systems involved in the load-sharing scheme is the home for the IP Phone. NUID cannot be at the home system for the IP Phone. This prevents additional redirections; that is, for the IP Phone redirected from the branch office, load sharing is not applied. If the home system fails, the IP Phone reregisters at the branch office. All this is due to the fact that backup, home, and branch office systems have different home location numbers.

For Controlled Load-sharing configuration to support the Branch Office feature, the home and backup systems must both be configured as the home office for the MG 1000B, according to the instructions in *Media Gateway 1000B: Installation and Configuration* (553-3001-214). For the MG 1000Bs to be redundant, each site must use the same TN and DN ranges for the MG 1000B IP Phones.

Figure 25 on [page 113](#) shows an MG 1000B installed in the Controlled Load-sharing configuration.

Figure 25
Controlled Load-sharing configuration: Branch Office support



553-AAA2218

The MG 1000B can be configured as survivable in conjunction with the Controlled Load-sharing configuration. In the unlikely event that both home and backup systems fail, the MG 1000B reverts to survivable.

NRS Routing for Branch Office

As the MG 1000B can operate with either the home or backup system functioning as the main office, the NRS must be configured to redirect MG 1000B IP Phones to the appropriate active system.

Note: To redirect IP Phones to the main office, the MG 1000B uses the IP Phone's Branch User ID (BUID) value (configured in LD 11).

The NRS must also be configured to properly route incoming UDP, CDP, and VNR calls when the MG 1000B IP Phones are registered to the home system, to the backup system, or to the Branch Office.

UDP

When the MG 1000B IP Phones are registered on the home or backup system, the NRS definitions required to properly route incoming UDP calls are the same as those described in "UDP calls and IP Phone registration redirection" on page 110. Specifically, on the NRS, the HLOC for the home system and backup system endpoints must be defined with the least-cost factor.

In the unlikely event that both the home and backup systems fail, an additional NRS definition is required to ensure survivability of the MG 1000B. The branch office HLOC must be defined on the branch office endpoint with the least-cost factor. This additional entry ensures that UDP calls can reach the MG 1000B when the home and backup systems are both unavailable.

Note: Since the HLOC value at the branch office is different than the HLOC value of the home and backup systems, the UDP dial-in number to the MG 1000B IP Phones is different when both main office systems fail.

CDP and VNR

When the MG 1000B IP Phones are registered on the home or backup system, the NRS definitions required to route incoming CDP calls to the IP Phones are similar to those described in "CDP and VNR calls" on page 111. Specifically, the range of main office DNs used for the Branch Office IP Phones must be configured on the NRS as least-cost for the home system

and higher-cost for the backup system. This ensures that incoming CDP calls to the MG 1000B IP Phones are routed to the active home system.

These CDP entries also support the VNR call rerouting coming from the MG 1000B.

In the unlikely event that both the home and backup systems fail, a third NRS definition is required to ensure survivability of the MG 1000B. The same DN range must be defined on the branch office endpoint with a higher cost factor than the home and backup system endpoints. This entry ensures that CDP calls are rerouted to the MG 1000B when the home and backup systems are both unavailable.

BUID redirections with CDP

To support the Branch Office feature in the Controlled Load-sharing configuration, the BUIDs must be based on the CDP dialing plan, (that is, BUID = DN).

Note: As the home and backup systems have different HLOC values, the Controlled Load-sharing configuration does not support UDP-based BUIDs.

As a result, the routing entry on the NRS used to route incoming CDP calls also supports registration redirection requests for the MG 1000B. When the MG 1000B queries the NRS with the BUID to determine the home system of the IP Phone, the NRS responds with the active home system: home or backup.

Installing a Controlled Load-sharing configuration

Procedure 14 describes the high-level steps required to install a Controlled Load-sharing configuration.

Procedure 14

Installing Controlled Load-sharing configuration

- 1 Install or upgrade each system to the appropriate software.
- 2 Configure the two systems for IP Peer Networking, with a Primary NRS and Alternate NRS. See *IP Peer Networking: Installation and Configuration* (553-3001-213) for details.
- 3 Configure your IP Phone DNs and TNs at both sites.
- 4 At each backup site, configure the appropriate NUID and NHTN values for the redundant IP Phones, as well as Vacant Number Routing.
- 5 For each redundant IP Phone, configure the appropriate Connect Server values (S1 and S2).

End of Procedure

Provisioning the IP Phones

To install and configure IP Phones, see *Communication Server 1000E: Installation and Configuration* (553-3041-210). Ensure the S1 of the redundant IP Phone points to the backup system node TPS and S2 points to the home system node TPS.

To configure IP Phones using Dynamic Host Configuration Protocol (DHCP), see *Data Networking for Voice over IP* (553-3001-160).

The NUID and NHTN must also point to their home system. Configure the NUID and NHTN values on the backup system in LD 11 as follows:

LD 11: Configure NUID and NHTN

Prompt	Response	Description
REQ	NEW/CHG	Add new data or change existing data
TYPE	i2001/i2002/ i2004/i2050	IP Phone type.
CUST		Customer number.
	0-99	Range for CS 1000M Large System and CS 1000E.
NUID		Network User ID: Dialable home system DN.
	aaaa	Network User Id. Enter X to delete.
NHTN		Network Home TN: home system TN.
	l s c u	Format for CS 1000M Large System and CS 1000E where l = loop, s = shelf, c = card, u = unit.

OTM 2.2

The NUID and NHTN values can also be configured using OTM.

When using OTM Station Administration for IP Phones, it is possible to copy and paste an IP Phone from one system to another. This can be useful for provisioning the IP Phone data on both the home system and backup system.

Maintenance

The home and backup systems conform to the methods and procedures used for local and remote access, as defined for CS 1000M Large Systems and CS 1000E systems.

Geographic Redundancy implementation preserves all existing VxWorks or Overlay support tools available on the CS 1000M Large System or CS 1000E solutions, except where enhancements are noted in this NTP.

OTM 2.2

OTM 2.2 can be used to administer the home and backup systems in a Controlled Load-sharing configuration. The home and backup systems are represented in OTM as separate systems. System-specific changes made on one system (such as IP addresses and Event Preference Table [EPT] definitions) do not affect the other system.

Configuring the Database

During normal operation, each system is the master of its own customer database. Perform all database modifications on each system separately, by direct administration or through OTM.

Note: Both customer databases in the Controlled Load-sharing configuration are configured and updated manually. There is no database-replication process involved.

If all the offered features and services are required to be redundant, the backup system must be configured appropriately, and each change that is made on one system must be reflected on the other system.

IP Phone Test Local Mode

The IP Phone Test Local Mode can be used with the Controlled Load-Sharing configuration to register an IP Phone to its backup system. For more details, refer to “IP Phone Test Local Mode” on page 87.

Feature interactions

The redundant features available to an IP Phone are limited to the features that are offered on its backup system.

System monitoring

Nortel recommends implementing SNMP alarm management to monitor the health of home and backup systems. SNMP can be used to trigger alarms, for

example, when any IP Phone unregisters from a system. For more information, see *Simple Network Management Protocol* (553-3001-519).

Geographic Redundancy N+1 configuration

Contents

This section contains information on the following:

Description	121
Planning	124

Description

The N+1 configuration increases the reliability of CS 1000M Large Systems (CP PII and CP PIV) and CS 1000E systems through configuration of a geographically remote system that operates as a backup for multiple systems. Figure 26 on [page 123](#) shows one CS 1000E system backing up two others in a N+1 configuration.

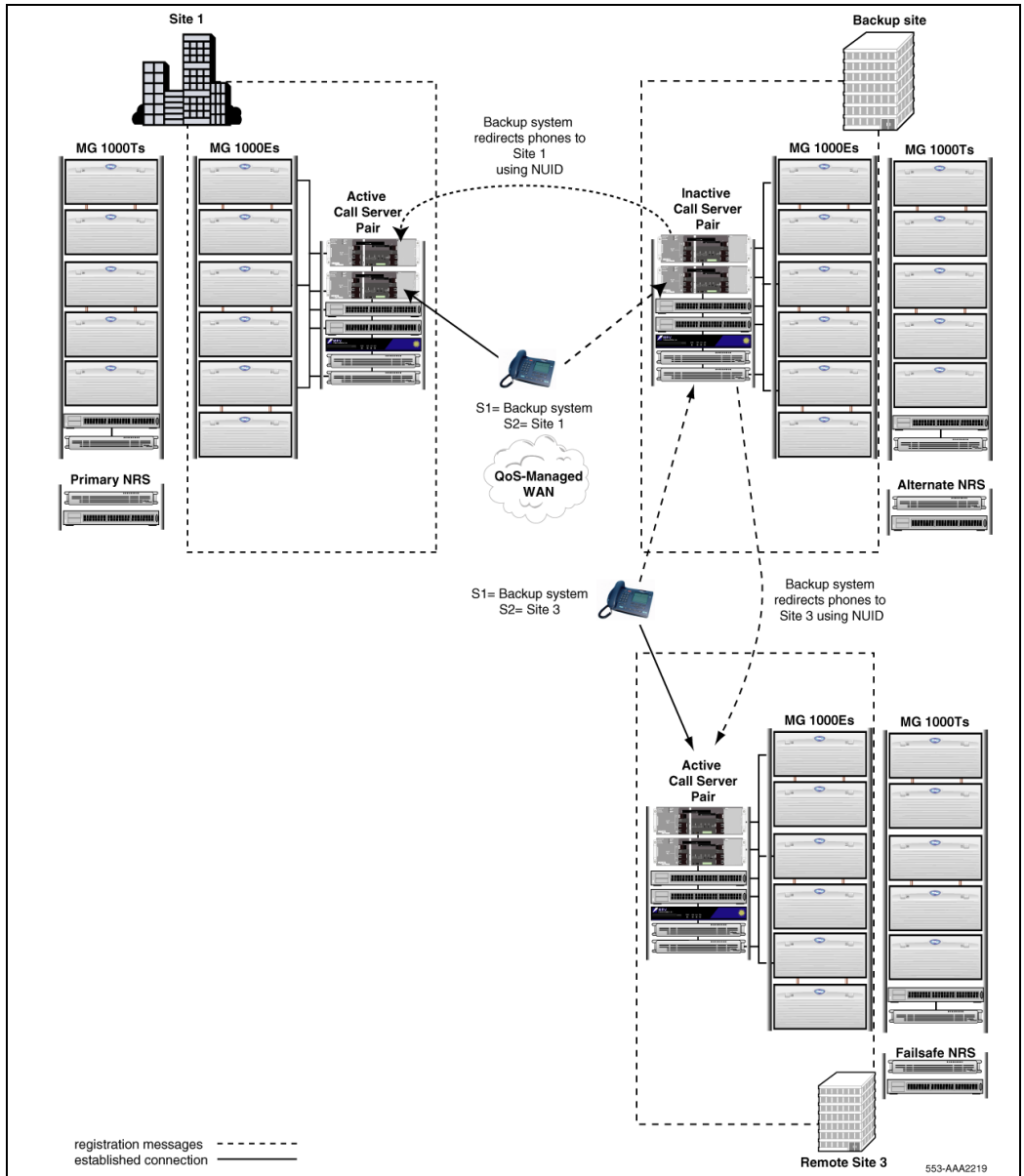
In the N+1 configuration, the backup system provides redundancy for the Site 1 and Site 3 systems. The backup system is equipped with the GRSEC package, allowing it to operate as a dedicated standalone system and provide state transition in the same manner as the 1+1 configuration. However, as the N+1 configuration provides redundancy for multiple systems, it does not support database replication. Therefore, the backup system does not have to be of the same system type as either the Site 1 or Site 2 systems.

Note: The GRSEC package (405) must be equipped during the software installation process; it cannot be added using a new keycode post software installation.

The N+1 redirection process is similar to that of the Controlled Load-sharing configuration. All redundant IP Phones must have Network User ID (NUID) and Network Home TN (NHTN) values manually defined at the backup site.

Note: When the NUID is defined manually on the backup system, this overrides the automatic NUID generation of the GRSEC package (405).

Figure 26
N+1 configuration



The primary Connect Server (S1) of each redundant IP Phone points to the backup system. When an IP Phone powers up, it registers first with the backup site Terminal Proxy Server (TPS), then with the backup system itself. The backup system, reading the NUID of the IP Phone, automatically redirects the IP Phone to its appropriate home system, either Site 1 or Site 3, using the NRS.

If either home system fails, the backup system provides service to the affected IP Phones.

Software

To implement the N+1 configuration, the backup system must run CS 1000 Release 4.0 or later and must be equipped with the GRSEC package. The home systems must run Succession 3.0 software or later.

Note: The GRSEC package (405) must be equipped during the software installation process; it cannot be added using a new keycode post software installation.

Ideally, the software packages on the backup system must provide the same functionality as those offered on the home systems. However, this is not a necessity if less functionality is acceptable at the backup system.

Planning

In the N+1 configuration, each home system must be planned and installed in the same manner as a home system in the Controlled Load-sharing configuration. See “Planning a Controlled Load-sharing configuration” on page 106 and “Installing a Controlled Load-sharing configuration” on page 116 for details.

The backup system in the N+1 configuration follows the same planning and installation steps as the backup system in the Controlled Load-sharing configuration, but with some additional considerations. First, the backup system is equipped with the GRSEC package. As a result, the backup system State Control Block must be configured appropriately during installation. See “Configure Geographic Redundancy State Control Block in LD 117” on page 71 for details.

Second, the redundant IP Phones on the home systems must be defined using non-overlapping TNs. The TN ranges used for redundant IP Phones on one home system must not be used for redundant IP Phones at another home system. This ensures that, in the event that more than one home system fails, two IP Phones do not attempt to use the same TN at the backup system.

Finally, the backup system in the N+1 configuration must be planned based on the redundancy needs of multiple home systems. When planning the N+1 configuration, there are two failure scenarios to be considered:

- failure of the home system that demands the most redundancy resources from the backup system
- failure of all home systems at once

At minimum, plan the backup system in the N+1 configuration such that it has enough resources to provide the required redundancy during failure of the system demanding the most capacity.

The practical maximum is to plan the backup system to provide redundancy during the failure of all home systems.

Within these limits, the administrator is free to determine how much redundancy is desired. The decisions vary for different N+1 configurations and are based on the statistical evaluations of probability of different failure scenarios.

Campus Redundancy

Contents

This section contains information on the following topics:

Description	128
High Speed Pipe (HSP) IP address management enhancement....	129
“Stop and Copy” protocol enhancement	129
Operating parameters	130
Normal Operations	130
Network topology	135
Third-party vendor switching equipment.....	139
Call Server operation during IP network failure.....	140
ELAN subnet connectivity between the CPUs is lost but HSP is still operational	140
HSP connectivity is lost but ELAN subnet connectivity between the CPUs is operational	140
ELAN subnet and HSP connectivity is lost between the CPUs....	141
HSP configuration.....	141
Initial installation	141
High Speed Pipe IP address configuration.....	143
HSP recommendations and rules	141
IP Telephony node configuration.....	149
Upgrading a redundant system	150
Downgrading a redundant system.....	152
HSP maintenance	153
STAT CPU	153

STAT ELNK	157
Troubleshooting	158

Description

The Nortel Networks Communication Server (CS) 1000E system is a highly-scalable and robust IP PBX that offers support of IP-based applications using industry-standard SIP and H.323 interfaces, while providing an industry-leading set of telephony features and applications.

The Campus Redundancy feature provides the ability to separate the CS 1000E Call Servers in a campus environment for “campus mirroring”. This feature enables two Call Servers, one active and one redundant, to be connected through an Ethernet network interface. CS 1000 Release 4.5 provides enhancements to the CS 1000E system to allow campus mirroring to operate using other vendors’ switching products in addition to the BayStack 470. See “Third-party vendor switching equipment” on page 139.

To separate the redundant Call Servers, the ELAN subnet and the subnet of the High Speed Pipe (HSP) may be extended between the two processors using networking equipment that provides layer 2 end to end connectivity.

Note: Campus Redundancy is not supported for CS 1000M Large Systems.

The Campus Redundancy enhancements, in release 4.5, change the operation of the High Speed Pipe (HSP), which is the interface that is used to provide:

- synchronization of the redundant Call Server’s disk and memory subsystems
- sharing of “Health” information
- memory shadowing between the two Call Servers during graceful switchover operations.

The HSP uses one of the network interfaces on each of the CPUs. The HSP port is labelled “LAN 2” on the faceplate of the processor.

Note: Contact the Nortel representative for information on the latest supported products.

If the two Call Servers are collocated, the HSP can be connected using a standard CAT5e or CAT6 crossover cable, limited to 100 meters in length.

High Speed Pipe (HSP) IP address management enhancement

Prior to release 4.5, the existing IP addresses assigned to the HSP ports are fixed addresses that are not configurable by customers.

The Campus Redundancy enhancement, in release 4.5, allows IP addresses to be configured for the HSP that do not conflict with other addresses in the customer's enterprise IP networks.

These addresses are provisioned against a specific CPU (side 0 or side 1). Optionally, you may choose not to configure the HSP IP addresses and in this case the HSP interfaces use the following default IP addresses:

- 1** 127.2.0.1 is bound to the Side 0 CPU.
- 2** 127.2.0.2 is bound to the Side 1 CPU.

When configuring a HSP in which the CPUs are connected through a data network, the IP addresses must be configured for each CPU/Side so that address conflicts can be avoided within the IP network.

“Stop and Copy” protocol enhancement

The existing “Stop and Copy” protocol is used during a graceful switchover between CPUs. The switchover can be due to a manual request, midnight maintenance routine, or a health count mismatch between the two CPUs during regular traffic periods.

This release 4.5 enhancement changes the “Stop and Copy” protocol to use standard Layer 3 and Layer 4 protocols (IPv4 packet type at Layer 3 and UDP packet type at Layer 4). The Layer 2 header is modified to reflect that the payload is now IPv4. This allows the protocol to be carried through standard data networking products. It ensures that the protocol used on the IP network

conforms to standard headers in order to avoid incompatibilities as the packets are transported.

Operating parameters

The use of VLAN configurations and port priority settings to protect the ELAN and HSP network interfaces from harsh network conditions is required to ensure reliable operation. This minimizes the risk of unexpected network problems, such as heavy traffic conditions, broadcast storms, network stress caused by a virus, and Denial of Service attacks.

Fast Spanning Tree Protocol Learning (or disabling of Spanning Tree altogether), physical port-based priority, and VLANs must be supported by the networking products used to carry the HSP traffic. Nortel recommends Multi-link Trunking to provide redundancy in the connections between CS 1000E CPU locations.

Refer to “HSP configuration” on page 141 for details on the operating parameters.

Normal Operations

During normal operation the active and redundant CPUs are both running in parallel. . The difference between the two CPUs is that the active side is running call processing applications while the redundant side is running only diagnostics and management tasks.

The redundant CPU can take over from the active CPU in certain conditions. The Campus Redundancy feature allows for a second “redundant” call server to take over from the “active” call server in certain conditions. System operation under Campus Redundancy is similar to the existing CP PII and CP PIV redundant call processor operations. During normal functioning, one Call Server is in active mode and the other is in redundant mode. The active Call Server’s protected memory and disk subsystems are shadowed to the redundant Call Server using a synchronization protocol over a the 100BaseT HSP interface. This ensures that the redundant Call Server can assume system control in case of failure of the active Call Server.

Depending upon the situation a graceful switchover or an ungraceful switchover may occur. The active CPU becomes redundant and the redundant CPU becomes active.

Disk shadowing also allows for a graceful switchover, where system control can be switched from the active to the redundant CPU Call Server, while maintaining all call state information with only a brief pause (several seconds). The switchover can be performed once a day, during the midnight routines. This ensures that both Call Servers are fully capable of supporting call processing operations. Any failure in this switchover is reported with an error message and SNMP alarm, so that the problem can be corrected before becoming a hidden second point of failure.

Graceful switchover can also be performed manually to facilitate maintenance operations and software upgrades.

The two Call Servers also use the HSP to communicate their individual status (active or redundant) to each other. In addition, a health count is maintained within each Call Server for critical components such as disk drives, physical 100BaseT LAN ports, and connectivity to the other devices on the ELAN subnet. The health count is communicated between the two Call Servers and is used to detect whether one processor is healthier than the other.

The following sections describe the operation in more detail.

Warmstart and Coldstart

Warmstart

This recovery mechanism involves restarting the entire Operating System on the Control Processor. All tasks are restarted. The call processing task (tSL1) executes the INITIALIZE procedure. Basically, all its protected configuration data is preserved (ie, not reloaded from hard drive) and the task will rebuild all the unprotected data. In addition, established calls are rebuilt in the INITIALIZE procedure.

Coldstart

This recovery mechanism involves restarting the entire Operating System. All tasks are restarted including the tSL1 task. The tSL1 task executes the

SYSLOAD procedure. Basically, protected data is all cleared. Configuration data is reloaded from the hard drive and rebuilt into the protected data.

Fault Detection

Software watchdog mechanism

Important tasks are registered with the software watchdog task. The registered task has to "punch" the software watchdog periodically; otherwise, the corresponding software watchdog times out. In general, if the watchdog timer for a registered task times out twice consecutively, the registered task is restarted. If the task has been restarted 15 times, a system warmstart will be invoked.

Hardware watchdog mechanism

A hardware watchdog is the defensive mechanism against processor runaway or a high priority task consuming all CPU cycles. If the hardware watchdog times out the first time, it will trigger a system warmstart. If the warmstart process cannot reset the hardware watchdog, the second hardware watchdog will trigger a system coldstart.

Exception handling

When a processor exception occurs, the exception handler will analyze the cause of the exception and the context in which the exception is invoked. If a task causes an exception, the task is restarted. If the exception is from tSL1, system warmstart is invoked.

Health Monitoring

Each Call Server possesses a health count (available via the STAT HEALTH or STAT CPU command in overaly 135). The Health State of each Call Processor Unit (CPU) is an indication of the current operating state of all the major hardware components in the network. Each component is assigned a health count based on the current operating state. The overall CP health measure is the sum of the health counts of all the components. As such, the CP health measure depends on the system configuration.

Switchover

Graceful Switchover

In normal operation the health count of each CPU should be equivalent. In the case where the active CPU detects that the redundant CPU has better health, a graceful switchover is invoked. In this process, almost the entire memory image from the active CPU is copied over to the memory of the redundant CPU. Then the redundant CPU will resume the operations left off from the active CPU after going through a post-switchover procedure. This post-switchover procedure includes sending out a gratuitous ARP message to the IP world for informing where the active IP ELAN address is located. This CPU then becomes the active side.

The previously active side will invoke a warmstart after the copying operation is completed. After the warmstart, it will become the redundant side.

During a graceful switchover there should be no impact to calls already in progress. There will be a brief duration whereby new calls will not be allowed in the neighborhood of 6-8 seconds depending upon the configuration.

Graceful switchover may be invoked manually using the SCPU command in overlay 135.

Ungraceful Switchover

Once it is decided that the active side is inoperable (e.g. power or processor failure, watchdog timeout, exceptions), the redundant side will warm start and take over control. The switchover will not occur immediately, since once the redundant side detects loss of heartbeat, it must wait long enough to be sure that the active side is not simply performing a warm start (INI). The timer used to invoke the ungraceful switchover is in the order of 56 seconds.

Midnight Switchovers

Because of the robustness of the new call processor architecture, the need to perform CPU switchovers during midnight routines are no longer required and have been removed from the software routine. With Call Processor PII and Call Processor PIV, both CPUs are alive (although only one is in call processing state).

It is still possible to have a daily switchover of the CPUs during the midnight routine if so desired.

IMPORTANT!

Nortel's recommendation:

- 1 If the customer can tolerate a service interruption of 6 to 10 seconds during the daily diagnostic routines which are normally scheduled outside of business hours (nominally "midnight"), and if the system is monitored daily or in real time for critical alarms, then the daily scheduled switchover of active CP side is recommended.
- 2 If the customer cannot tolerate a daily scheduled diagnostic test, then a CP side switchover test should be conducted during a scheduled maintenance window at least once a year, and preferable monthly or quarterly.
- 3 Never switching active CP side is not recommended, because a hardware fault on the inactive standby CP side may not be discovered until the active side experiences a hardware failure, a power failure, or a network connection failure.

These recommendations apply to all dual processor machines.

The following steps are required to provision the midnight switchover.

- LD 17
- REQ chg
- TYPE ovly
- DROL 135
- MID_SCPU yes

Impact on calls

Depending upon whether the switchover is graceful or ungraceful there may be an impact to calls. In order to determine what the impact of the switchover has on calls please refer to *Data Networking for Voice over IP* (553-3001-160).

Generally, established basic calls survive both the graceful and ungraceful switchovers. Basic calls that are in a transient state (ie. calls that are in the dialing state) survive a graceful switchover but do not survive an ungraceful switchover.

Heartbeat

The two CPUs exchange heartbeats in order to determine if the other CPU is reachable over the HSP. The heartbeat protocol also carries information regarding the health count of each CPU.

If the HSP is disconnected then the heartbeat protocol attempts to traverse the ELAN instead.

If the heartbeat cannot be communicated between the two CPUs meaning that connection over the HSP and ELAN is lost between the two CPUs then the redundant CPU will warmstart to become active after a certain period of time.

Network topology

The CS 1000E system provides the ability to distribute the redundant Call Server CPUs to two locations.

The initial offering of this feature in RIs 4.0 made use of dark fiber driven directly by BayStack 470 Layer 2 switches. This allowed the CS 1000E redundant Call Servers to be distributed to two locations that are separated by as much as 40 km. This configuration, see Call Server and Signaling Server (HSP and ELAN subnet) separated with Layer 2 switching products¹³⁷, is still supported as the base offering. The Campus Redundancy enhancements starting in RIs 4.5 supports any vendor's switching product, providing an installation test is run to measure packet loss, jitter, and delay.

Baystack 470 GBIC Fibre Interfaces

The Campus Redundancy feature is supported in the RIs 4.0 timeframe using Baystack 470 Layer 2 switches only as the transport mechanism between the 2 system cores.

Any of the Baystack GBIC interfaces can be used as long as the interface specifications are met for cable type, length and attenuation. The following are different Baystack 470 GBIC's available.

- 1000BASE-SX on MultiMode Fiber (50 μ m) 550 m
- 1000BASE-SX on MultiMode Fiber (62.5 μ m) 275 m
- 1000BASE-LX on MultiMode Fiber (50 μ m) 550 m
- 1000BASE-LX on MultiMode Fiber (62.5 μ m) 550 m
- 1000BASE-LX on SingleMode (9 μ m) 5 km
- 1000BASE-XD on SingleMode (9 μ m) 40 km

Campus Redundancy Baystack 470 Bandwidth Use

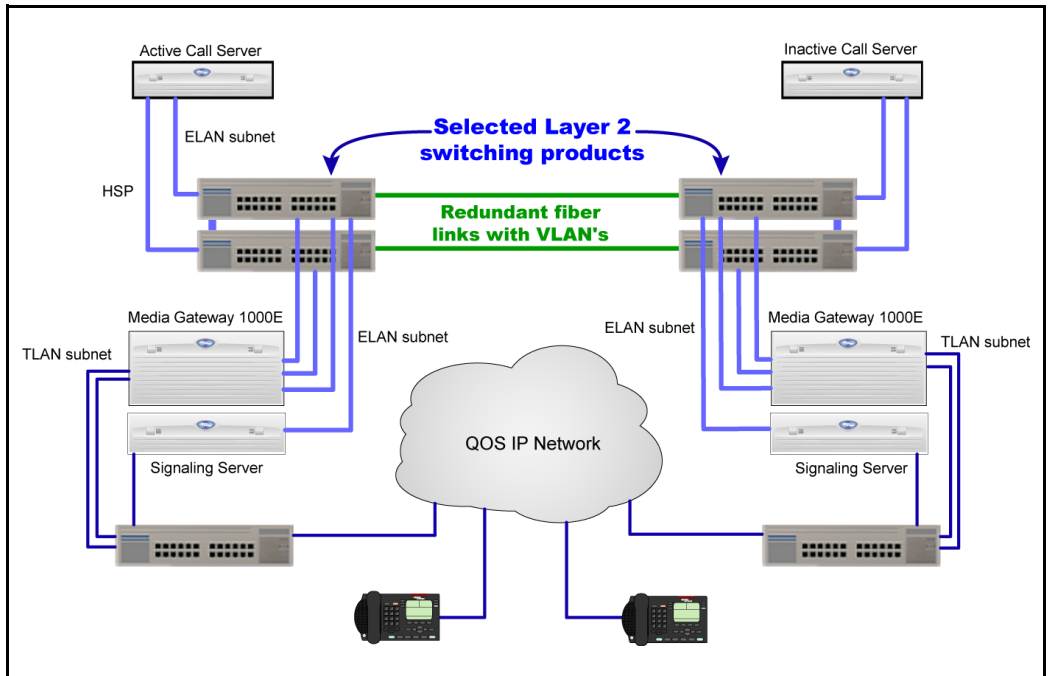
The Communication Server 1000E ELAN and HSP Ethernet links each require a dedicated 100 Mbps VLAN on the Baystack 470 1Gbps link. Although not specifically stated in the NTP's, the remainder of the Baystack 470 1Gbps Fiber link (800 Mbps) can be used for other data.

The requirements to use this extra bandwidth include:

- The extra bandwidth must be configured on a VLAN separate from the ELAN and HSP VLAN's
- The ELAN and HSP VLAN's must be set up with higher priority than the other VLAN's to ensure they get bandwidth when required for an HSP call server switch over.

Nortel recommends that the actual configured aggregate bandwidth for the extra data traffic not exceed 800 Mbps. This will further ensure that the ELAN and HSP ports always have enough bandwidth to complete their tasks.

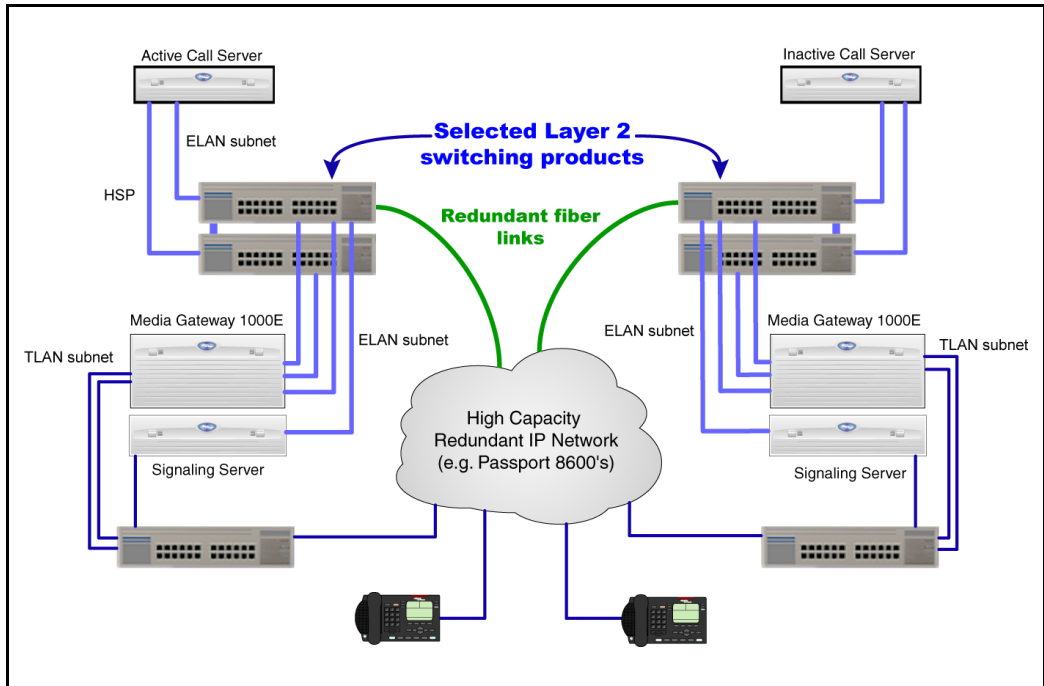
Figure 27
Call Server and Signaling Server (HSP and ELAN subnet) separated with Layer 2 switching products



In addition, various other network topologies are supported that allow converged voice and data traffic to share the links between locations. However, the network design must include mechanisms such as priority, isolated VLANs, and other robust design principals to ensure that the network design meets stringent requirements for packet loss, delay, and other network characteristics.

Figure 28 on page 138 illustrates an alternative network topology that supports the Campus Mirroring of CS 1000E CPUs.

Figure 28
Call Server and Signaling Server (ELAN subnet and HSP) separated by high capacity network



Note: Nortel recommends that Node Terminal Proxy Server (TPS) Signaling Servers be distributed between the two sites to prevent the system from disabling, in case of any local disaster in a single site (that might trigger failure of TPS registration). Configure the Signaling Servers in both sites in a single node to enable load balancing between all Signaling Servers in the system.

Switching Equipment

Layer 2 switching equipment

The following equipment supports both the MLT (Multi Link Trunking), port based VLANs, and 802.1P priority configuration and is recommended for the HSP application.

- 325-24T - Layer 2 VLANs, MLT, 802.3ad
- 325-24G - Layer 2 VLANs, MLT, 802.3ad
- 425-24T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 425-48T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 460-24T-PWR - Layer 2 VLANs, MLT, DMLT, , 802.3ad, 802.3af PoE
- 470-24T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 470-48T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 5510-24T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing
- 5510-48T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing
- 5520-24T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing, 802.3af PoE
- 5520-48T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing, 802.3af PoE
- 8300 - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing
- 8600 - Layer 2 VLANs, MLT, DMLT, SMLT, 802.3ad, L3 interVLAN routing

Third-party vendor switching equipment

The HSP supports any vendor's switching equipment.

The following third party equipment has been tested:

- CISCO WS-3750G 24T-E GE ENH MULTILAYER CATALYST (Layer 2 VLAN mode)
- 3C17203-3COM US/ 3COM 24-PORT 10/100TX SWITCH W/2
- 3COM 3C17304-US 3COM SS3 SWITCH 4228G 28PORTS EN
- 13240 EXTREME SUMMIT 200-24 SWITCH - 24 PORTS

Note: The HSP cannot be routed. This means that the HSP cannot be extended through a layer 3 router unless that device supports a method of providing layer 2 end to end connectivity ie. layer 2 tunnelling. Therefore, when passing through routing equipment, the HSP must remain in the same subnet from one Call Server to the other (for example, tunneling the HSP over the network).

Call Server operation during IP network failure

The following section describes the operation of the CS 1000E system during various failure scenarios, and how the system recovers after the network is properly restored.

ELAN subnet connectivity between the CPUs is lost but HSP is still operational

In this scenario, only one CPU binds the primary ELAN network interface IP address to its network interface. The other CPU binds the secondary ELAN network interface IP address (no IP address conflict). All Media Gateway 1000Es are controlled by the CPU that has the primary ELAN network interface IP address. However, the Signaling Servers and Voice Gateway Media Cards are included in the health count of the CPUs, and each of these attempt a connection to both the primary ELAN network interface IP address and the secondary ELAN network interface IP address.

It is possible that, within minutes, the health counts of the CPUs can change, so that the CPU with the largest number of possible connections to ELAN devices has a higher health count than the other CPU. This causes a CPU switchover to occur, again with only one CPU binding the primary ELAN network interface IP address.

HSP connectivity is lost but ELAN subnet connectivity between the CPUs is operational

In this scenario, the same health count is calculated based upon connectivity (and other health count factors). This health information is now shared over the ELAN subnet. The CPUs are still redundant but memory and disk space are not synchronized between the active and redundant CPU.

ELAN subnet and HSP connectivity is lost between the CPUs

In this scenario, the subnet is split into two broadcast domains/segments, each holding one CPU and a number of Media Gateway 1000Es. Specifically, in this scenario. Each CPU attempts to talk to the other CPU. Once the HSP connection is restored then health information is exchanged. The CPU with the lower health count will reboot to become redundant.

In this case, the CPUs and Media Gateway 1000Es split into two independent systems, (each CPU is active) providing services to all their registered IP Phones and voice gateways, independent of each other. When a network connection is restored (either HSP or ELAN subnet), CPU 1 reboots and allows CPU 0 to resume complete control of all Media Gateway 1000Es.

Note: ARP is Address Resolution Protocol, the TCP protocol that translates an IP address into the MAC (physical hardware) address of the card. The ARP performs the address resolution.

HSP configuration

Initial installation

The HSP IP addresses are not configured during installation. Instead, they are configured in LD 117 after the system comes up. If HSP IP addresses have already been manually configured, then they are used as the system reboots. Otherwise, the default HSP addresses are used.

HSP recommendations and rules

The following are recommendations and rules for configuring the HSP network interface and network when using network equipment to connect the HSP network interfaces of the two Call Servers.

- The HSP must be connected through a cross-over cable or by a dedicated VLAN through switches.
- The HSP must be in its own IP subnet. It cannot be combined with the ELAN subnet.

- The minimum throughput of the HSP must be 100 Mbps. Therefore, the HSP port must be 100 Mbps and full duplex. This must be confirmed using the **STAT HSP** command in LD 137 after the equipment is operational. This must also be verified on the network equipment to which the HSP is attached.
- The network switches must be capable of port mapping to 802.1p/Q.
- When running the HSP across network equipment, the HSP must be isolated in its own VLAN. Do not include other traffic in this VLAN. This VLAN must be given higher VLAN priority than any other traffic on the network, except for network control traffic (network control traffic is the traffic necessary to keep the network operational). The VLAN must be 802.1p/Q-capable and must be set to a very high setting so as not to starve the HSP. Nortel strongly recommends 802.1p Level 7 (Network Control and OAM).
- When using third-party vendor network equipment that has not been validated by Nortel, a pre-test of the network must be performed. This test includes mixed traffic going across the networks in different VLANs. The network specifications should meet the round trip delay and packet loss requirements.
- The round trip delay of the HSP VLAN must be less than 30 msec and the packet loss of the HSP VLAN must be below .1 % packet loss. See “Customer validation” on page 149.

- The HSP port on the CPP4 is set to auto-negotiate the link speed and duplex. Therefore, the network equipment to which the CPP4 is attached must also use auto-negotiate. Verify that both the CPP4 and the network equipment speed and duplex are a match. The CPP2 does not auto-negotiate; instead, it is fixed to 100 Mbps and full-duplex. Verify that both the CPP2 and the network equipment speed and duplex is a match.
- Nortel recommends that MLT (Multi Link Trunking) be used across the enterprise IP network for the Campus Redundancy configuration.

**CAUTION**

Duplex mismatches occur in the LAN environment when one side is set to Auto Negotiate and the other is hard configured.

The Auto Negotiate side adapts only to the speed setting of the fixed side. For duplex operations, the Auto Negotiate side sets itself to half-duplex mode. If the forced side is full-duplex, a duplex mismatch occurs.

High Speed Pipe IP address configuration

The configuration of High Speed Pipe (HSP) IP addressing can optionally be performed after the installation process, if the default IP addresses are not appropriate for the customer network. Nortel strongly recommends allocation of a network IP address within the customer's address space, if the network is not dark fiber-driven by BayStack470 switches.

Existing configuration procedures are used to provision these IP addresses. Specifically, Host Names are used to identify the HSP ports IP addresses. The names used are:

- DEV_SIDE0_HSP - host name for the HSP on the Side 0 CPU
- DEV_SIDE1_HSP - host name for the HSP on the Side 1 CPU

The HSP IP addresses do not have to be manually configured. They can still negotiate to default IP addresses automatically.

CPU Side 0 = 127.2.0.1

CPU Side 1 = 127.2.0.2

Note that the addresses are specific to a particular side.

The only exception to this rule is when upgrading from CS 1000 Release 4.0 to CS 1000 Release 4.5. In this case, the CPU negotiates using the Release 4.0 scheme. After both sides are upgraded to Release 4.5 software, then the HSP IP addresses are the defaults of 127.2.0.1 and 127.2.0.2

The host names are not configurable; however, their parameters are configurable in LD 117. Changes to host name parameters require the use of the **out** and **new** commands; the **chg** command is not allowed.

Note: The HSP IP addresses and subnet mask are not activated until the SET HSP_IP command is used or the CPU reboots.

Note: The CPU should not be rebooted after changing but before issuing the SET HSP_IP command. Doing so may cause the HSP addresses between the active CPU and the redundant CPU to become out of sync.

Example of HSP configuration

=> new host DEV_SIDE0_HSP 192.168.100.10

INET Data Added

=> new host DEV_SIDE1_HSP 192.168.100.11

Warning: HSP Subnet Mask not configured. Please enter HSP Subnet mask using the CHG HSP_MASK command

INET Data Added

=> chg hsp_mask 255.255.255.252

INET Data Changed

=> prt host

Call Server

ID	Hostname	IP Address
1	LOCAL_PPP_IF	137.135.192.4
2	REMOTE_PPP_IF	100.1.1.1
3	ACTIVE_CPU	47.11.226.10
4	INACTIVE_CPU	47.11.226.11
7	DEV_SIDE0_HSP	192.168.100.10
8	DEV_SIDE1_HSP	192.168.100.11

=> prt hsp_mask

HSP SUBNET MASK: "255.255.255.252"

OK

=> set hsp_ip

Activating HSP Addresses. Please wait ...

System is Redundant. Rebooting Inactive side to activate new HSP IP addresses ...

24/03/2005 01:03:31 SRPT0118 CM: Server connection lost.

SRPT118 CM: Server connection lost.

Side 0 HSP IP set to "192.168.100.10"

Side 1 HSP IP set to "192.168.100.11"

HSP subnet mask set to "255.255.255.252"

OK

HSP IP address commands

The NEW HOST command is used to configure the HSP IP addresses.

Syntax:

NEW HOST DEV_SIDE0_HSP <ip address>

or

NEW HOST DEV_SIDE1_HSP <ip address>

The PRT HOST and OUT HOST commands are used to display and remove the host entries for HSP ports.

HSP subnet mask commands

The HSP subnet mask must be configured in LD 117 if the HSP IP addresses are configured. Three commands are available:

- CHG HSP_MASK
- OUT HSP_MASK
- PRT HSP_MASK

Table 5 describes the LD 117 HSP subnet mask commands.

Table 5
LD 117 HSP subnet mask commands

Command	Description
CHG HSP_MASK <subnet mask>	Modifies the manually-configured subnet mask, if it exists; otherwise, the subnet mask to the Call Server is added

Table 5
LD 117 HSP subnet mask commands

Command	Description
OUT HSP_MASK	Removes the configured HSP subnet mask from the Call Server and replaces it with the default HSP subnet mask
PRT HSP_MASK	Retrieves the manually-configured HSP mask from the Call Server, if the mask exists, and displays it on the screen; otherwise, the default HSP subnet mask (255.255.255.0) is displayed

HSP IP address activation

The SET HSP_IP command is introduced to LD 117 to activate the HSP IP addresses and subnet mask.

Table 6
LD 117 HSP IP address activation command

Command	Description
SET HSP_IP	Activates the HSP IP addresses and subnet mask

The SET HSP_IP command first causes sanity checks to be performed on the configured HSP IP addresses and subnet mask. If the IP addresses and subnet mask are configured correctly, a warm Restart message is sent to the redundant side, if the system is redundant. Then the local HSP network interface is configured with the HSP IP address and subnet mask from the manually-provisioned parameters. Since the system is redundant, the HSP IP address parameters are copied to the redundant side, so that when the redundant side boots up, the new IP addresses and subnet mask are used.

If the system is not redundant, only the local interface is configured with the HSP IP address and subnet mask from the manually-configured values.

If the SET HSP_IP command is executed and the HSP IP addresses and subnet mask are the same as the IP addresses and subnet mask already in use, then this command has no effect.

HSP status command

The PRT HOST and PRT HSP_MASK commands print the configured values of the HSP IP address and subnet mask. These values are not necessarily the HSP IP address and subnet mask in use on the Call Server. These values are not applied until the SET HSP_IP command is issued successfully.

To determine the current HSP IP address and subnet mask in use on the Call Server, the STAT HSP command is introduced in LD 137.

Table 7
LD 137 status command

Command	Description
STAT HSP	Displays the current HSP IP address and subnet mask in use on the Call Server

The following is an example of the output from a STAT HSP command.

```
.stat hsp
LCS HSP STATE is UP
HSP LINK CARRIER: OK
Auto Negotiation: Enabled
Auto Negotiation Completed: YES
Actual Line Speed: 100 Mbps
Actual Duplex Mode: Full Duplex

Ethernet (gei unit number 1):
Internet address: 192.2.3.11
Broadcast address: 192.2.3.255
Ethernet address: 00:c0:8b:07:bd:fd
Netmask: 0xffffffff00; Subnetmask: 0xffffffff00
415607 packets received; 680621 packets sent
0 input errors; 0 output errors
0 collisions
```


Customer validation

If the customer chooses to use network equipment between HSP ports, then the following must be done:

- Prior to installation, the network Service Level Agreement (SLA) for the HSP must meet minimum requirements.
- The network must meet the minimum requirements. See “HSP recommendations and rules” on page 141.
- Call processor graceful switchover must be tested after the CS 1000 installation.

IP Telephony node configuration

If there is a significant risk that the IP network could lose connectivity between the two Call Servers and their surrounding IP Telephony node devices, such as the Signaling Server and Voice Gateway Media Cards, then there is a possibility that such a split can cause two of those devices to attempt to bind to the same node IP address while the network is split. If the network segments are separated from each other, this should not cause a problem; but when the network is restored, it can take up to a minute for the node to elect a new node master and restore full operation. To avoid this situation, configure separate IP Telephony nodes at each physical location, when the Server settings (S1/S2) for IP Phones are both available for use.

If either S1 or S2 is being used for Geographic Redundancy or Survivable Branch Office, then each of the IP Telephony nodes can be registered with the Network Connect Server in the NRS with different cost factors, so that node redundancy is provided for these IP Phones as well.

Note: If the TLAN network interfaces provided by these devices are to be split into different subnets, they must be configured in separate nodes, or the network must provide a VLAN broadcast domain between the two locations. This is another reason to use separate nodes when using Campus Redundancy.

Upgrading a redundant system

The algorithm that negotiates the HSP IP address changes between CS 1000 Release 4.0 and Release 4.5. The Release 4.5 algorithm is backwards-compatible with the Release 4.0 algorithm, so that when one side of a redundant system is upgraded, the HSP pipe continues to function. When the remaining Release 4.0 Call Server is upgraded to Release 4.5 software, the new HSP algorithm takes effect and the HSP addresses are bound as described in “High Speed Pipe (HSP) IP address management enhancement” on page 129.

Note: When upgrading from Release 4.0 to Release 4.5 software, the HSP IP address must not be manually configured before upgrading both Call Servers to Release 4.5 software.

Table 8 gives an example of upgrading a redundant system from CS 1000 Release 4.0 software to Release 4.5 software.

Table 8
Example of upgrading system software (Part 1 of 3)

Command	CPU 0	CPU 1
	State = Active/ Redundant HSP IP = 127.2.0.2 S/W = 4.0	State = Inactive / Redundant HSP IP = 127.2.0.1 S/W = 4.0
Active side (CPU 0): SPLIT	State = Active / Split HSP IP = 127.2.0.2 S/W = 4.0	Cold Start to become split State = Inactive / Split HSP IP = 127.2.0.1 (w negotiation) S/W = 4.0

Table 8
Example of upgrading system software (Part 2 of 3)

Command	CPU 0	CPU 1
Inactive Side (CPU1): 1) upgrade to 4.5 S/W 2) reboot -1	No change	Cold Start State = Inactive / Split HSP IP = 127.2.0.1(w negotiation) S/W = 4.5
Active side (CPU 0): CUTOVR	State = Inactive / Split HSP IP = 127.2.0.2 S/W = 4.0	Warm Start to become Active State = Active / Split HSP IP = 127.2.0.1 (w negotiation) S/W = 4.5
Inactive Side (CPU 0): 1) upgrade to 4.5 S/W 2) reboot -1	Cold Start State = Inactive / Split HSP IP = 127.2.0.2 (w negotiation) S/W = 4.5	No change

Table 8
Example of upgrading system software (Part 3 of 3)

Command	CPU 0	CPU 1
Active side (CPU 1): JOIN	<p>Warm Start to become redundant</p> <p>State = Inactive / Redundant</p> <p>HSP IP = 127.2.0.1(w negotiation)</p> <p>S/W = 4.5</p>	<p>State = Active / Redundant</p> <p>HSP IP = 127.2.0.2 (IP address corrected when JOIN is issued)</p> <p>S/W = 4.5</p>
<p>Active Side (CPU 1):</p> <p>1) LD 117 – enter HSP addresses for both sides and optional subnet mask</p> <p>2) LD 117 SET HSP_IP</p>	<p>Warm Start</p> <p>State = Inactive / Redundant</p> <p>HSP IP=DEV_SIDE0_HSP (inet.db)</p> <p>S/W = 4.5</p>	<p>State = Active / Redundant</p> <p>HSP IP=DEV_SIDE1_HSP (inet.db)</p> <p>S/W = 4.5</p>

Downgrading a redundant system

It is possible to have a redundant system running CS 1000 Release 4.5 software with custom HSP IP addresses. When downgrading the software, one side (Call Server) reverts back to the default IP address and cannot talk to the other side. To avoid this situation, perform the following steps in the given order before performing the downgrade.

=> **prt host**

Call Server

ID	Hostname	IP Address
1	LOCAL_PPP_IF	137.135.192.4
2	REMOTE_PPP_IF	100.1.1.1
3	ACTIVE_CPU	47.11.226.10
4	INACTIVE_CPU	47.11.226.11
7	DEV_SIDE0_HSP	192.168.100.10

8 DEV_SIDE1_HSP 192.168.100.11

=> out host 7

=> out host 8

=> set HSP_IP

- split and downgrade

HSP maintenance

STAT CPU

The STAT CPU is available in overlay 135 and gives the status of both CPUs in a redundant configuration. This command is issued on the active CPU only and gives an indication of the redundant CPU on a best effort basis (e.g. if the system is not redundant the active side may not be able to communicate with the redundant side to get its status).

Definition of stat cpu results:

The first row indicates the state of the redundant system. It can be one of the following

- **TRUE REDUNDANT** - This means that both CPUs are up and actively communicating with each other. Disk and memory shadowing are complete.
- **SPLIT HSP DOWN** - The redundant system is split (the split command has been issued). Both CPUs are communicating over the ELAN but disk and memory shadowing between the two CPUs is not synchronized.
- **SPLIT HSP UP** - The redundant system is up but the system has been manually split by issuing the split command in overlay 135.
- **REDUNDANT HSP DOWN** - The system is redundant but the HSP is down. Both CPUs are communicating over the ELAN but the disk and memory shadowing between the two CPUs is not synchronized.
- **SYNCING** - The system is not redundant but disk and memorng shadowing between the two CPUs is in progress.

- SINGLE - The system does not have a redundant CPU or the ELAN and HSP to the redundant CPU has been disconnected.

DISK STATE. The second row indicates the intended state of the disk. It can be one of the following:

- DISK STATE = SPLIT - This indicates that the administrator has issued the SPLIT command in overlay 135.
- DISK STATE = REDUNDANT - This indicates that the administrator has issued the JOIN command in overlay 135.

HEALTH. The HEALTH indicates the relative health of each CPU. This number varies depending upon the system configuration. If either CPU experiences problems with hardware or connectivity to the network then the health count will go down.

Table 9
Overlay commands and results

Action	Result
JOIN command in overlay 135	<p>TRUE REDUNDANT DISK STATE = REDUNDANT HEALTH = 20 VERSION = Mar 22 2005, 15:21:44 Side = 1, DRAM SIZE = 256 MBytes</p> <p>TRUE REDUNDANT DISK STATE = REDUNDANT HEALTH = 20 VERSION = Mar 22 2005, 15:21:44 Side = 0, DRAM SIZE = 256 MBytes</p>
SPLIT command in overlay 135	<p>SPLIT HSPDOWN DISK STATE = SPLIT HEALTH = 20 VERSION = Mar 22 2005, 15:21:44 Side = 1, DRAM SIZE = 256 MBytes</p> <p>SPLIT HSPDOWN DISK STATE = SPLIT HEALTH = 20 VERSION = Mar 22 2005, 15:21:44 Side = 0, DRAM SIZE = 256 MBytes</p>
Disconnect the HSP	<p>REDUNDANT HSPDOWN DISK STATE = REDUNDANT HEALTH = 20 VERSION = Mar 22 2005, 15:21:44 Side = 1, DRAM SIZE = 256 MBytes</p> <p>REDUNDANT HSPDOWN DISK STATE = REDUNDANT HEALTH = 0 VERSION = Mar 22 2005, 15:21:44 Side = 0, DRAM SIZE = 256 MBytes</p>

Table 9
Overlay commands and results

Action	Result
SCPU command in overlay 135	<p>SYNCING DISK STATE = REDUNDANT HEALTH = 18 VERSION = Mar 22 2005, 15:21:44 Side = 0, DRAM SIZE = 256 MBytes</p> <p>SYNCING DISK STATE = REDUNDANT HEALTH = 20 VERSION = Mar 22 2005, 15:21:44 Side = 1, DRAM SIZE = 256 MBytes</p>
Disconnect HSP and ELAN	<p>REDUNDANT HSPDOWN DISK STATE = REDUNDANT HEALTH = 20 VERSION = Mar 22 2005, 15:21:44 Side = 0, DRAM SIZE = 256 MBytes</p> <p>REDUNDANT HSPDOWN DISK STATE = REDUNDANT HEALTH = 18 VERSION = Mar 22 2005, 15:21:44 Side = 1, DRAM SIZE = 256 MBytes</p>

STAT HSP

Use LD 137's STAT HSP command to monitor the HSP network interface.

The following is an example of Stat HSP output for a CP P4 processor (available only on the active side).

.stat hsp

LCS HSP STATE is UP

HSP LINK CARRIER: OK

Auto Negotiation: Enabled

Auto Negotiation Completed: YES

Actual Line Speed: 100 Mbps

Actual Duplex Mode: Full Duplex

Ethernet (gei unit number 1):

Internet address: 192.2.3.11

Broadcast address: 192.2.3.255

Ethernet address: 00:c0:8b:07:bd:fd

Netmask: 0xffffffff; Subnetmask: 0xffffffff

415607 packets received; 680621 packets sent

0 input errors; 0 output errors

0 collisions

STAT ELNK

The following is an example of the STAT ELNK command.

.stat elnk

ELNK ENABLED

Auto Negotiation: Enabled

Auto Negotiation Completed: YES

Actual Line Speed: 100 Mbps

Actual Duplex Mode: Full Duplex

Ethernet (gei unit number 0):

Host: PRIMARY_ENET

Internet address: 47.11.226.10

Broadcast address: 47.11.226.31

Ethernet address: 00:c0:8b:07:a5:9e

Netmask: 0xff000000 ; Subnetmask: 0xffffffe0

15 packets received; 20 packets sent

0 input errors; 0 output errors

0 collisions

New info

Troubleshooting

If one of the following problems occurs:

- the Call Servers do not perform graceful switchover and/or come up as single CPUs
- Disk sync and mem sync take a long time (greater than 10 minutes)

Then check the following:

- If it is a CP PIV processor, check the duplex and speed. Duplex mismatch is quite possible especially during an upgrade to CP PIV from CP PII using Baystack equipment. Duplex mismatch allows HSP to function, but packet loss will be great.
- If it is a CP PII processor, verify that the Speed and duplex of the LAN equipment connected to the HSP is hard-coded to 100 Mbps full duplex.
- If the HSP traverses a network of switches make sure that the HSP is on its own VLAN. Verify that the 802.1 priorities are configured properly.

Appendix A: Configuring the BayStack 470-24T for Campus Redundancy

Contents

This section contains information on the following topics:

Description	159
BayStack 470-24T configuration	161

Description

Table 10, Table 11, “VLAN port configuration,” on page 160, and Table 12, “MultiLink Trunk configuration,” on page 161 describe the configuration of the BayStack 470-24T VLANs.

Table 10
BayStack 470-24T VLAN assignment (Part 1 of 2)

VLAN Number	VLAN Name	VLAN Type	Port Membership
1	Default	Port-based	Switch 1- ports 1-26 (all) Switch 2- ports 1-26 (all) Switch 3- ports 1-26 (all) Switch 4- ports 1-26 (all)

Table 10
BayStack 470-24T VLAN assignment (Part 2 of 2)

VLAN Number	VLAN Name	VLAN Type	Port Membership
2	HSP	Port-based	Switch 1- port 1, port 25 (GBIC) Switch 2- port 25 (GBIC) Switch 3- port 1, port 25 (GBIC) Switch 4- port 25 (GBIC)
3	ELAN	Port-based	Switch 1- ports 2-24, port 25 (GBIC) Switch 2- ports 1-24, port 25 (GBIC) Switch 3- ports 2-24, port 25 (GBIC) Switch 4- ports 1-24, port 25 (GBIC)

In this configuration example, the following ports in the BayStack 470-24T switches are connected to Call Server ELAN network interfaces (in VLAN 3: ELAN):

- Switch 2 – port 24
- Switch 4 – port 24

Different network interfaces can be assigned to the BayStack 470-24T VLANs and connected to HSP and ELAN network interfaces on each Call Server. The configured VLAN network interfaces must match the physical connections.

Table 11
VLAN port configuration

Switch Number	Port Number	PVID (Port VLAN Identifier)	Tagged Member
Switch 1	1	2	No
	2-24	3	No
	25-26	1	Yes

Table 11
VLAN port configuration

Switch Number	Port Number	PVID (Port VLAN Identifier)	Tagged Member
Switch 2	1-24	3	No
	25-26	1	Yes
Switch 3	1	2	No
	2-24	3	No
	25-26	1	Yes
Switch 4	1-24	3	No
	25-26	1	Yes

Table 12
MultiLink Trunk configuration

Trunk	Trunk Members [Unit /Port]
1	[1 / 25] [2 / 25]
2	[3 / 25] [4 / 25]

Note: The four remaining high-speed fiber uplinks (GBIC ports 26) are not used in this configuration. They can be optionally used for MLT by being added to the existing uplink fiber network interfaces (ports 25), or for other dedicated uplink connectivity to network core switches.

BayStack 470-24T configuration

Procedure 15 must be performed for the switch stacks at both Call Server sites.

Procedure 15

Configuring the BayStack 470-24T using web-based management

- 1 From the main menu of the BayStack 470-24T web-based management interface, choose **Configuration > Port Management**.
- 2 Configure the HSP network interface on switch 1 (and 3) as shown in Figure 29 on [page 162](#).

Figure 29
HSP port configuration

Configuration > Port Management

Port Management Setting

Unit **1** 2

Port	Alias	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
1	HSP- side1		Enabled ▾	Up	On ▾	Disabled ▾	100Mbps / Full ▾
2			Enabled ▾	Down	On ▾	Enabled ▾	▾
3			Enabled ▾	Down	On ▾	Enabled ▾	▾
4			Enabled ▾	Down	On ▾	Enabled ▾	▾
5			Enabled ▾	Down	On ▾	Enabled ▾	▾
6			Enabled ▾	Down	On ▾	Enabled ▾	▾
7			Enabled ▾	Down	On ▾	Enabled ▾	▾
8			Enabled ▾	Down	On ▾	Enabled ▾	▾
9			Enabled ▾	Down	On ▾	Enabled ▾	▾
10			Enabled ▾	Down	On ▾	Enabled ▾	▾

- 3 Configure the GBIC network interface on switch 1 (and 3) as shown in Figure 30.

Figure 30
GBIC port (1) configuration

NORTEL NETWORKS

Access (RW)

- Summary
- Configuration
 - IP
 - System
 - Remote Access
 - SNMPv1
 - SNMPv3
 - SNMP Trap
 - MAC Address Table
 - Find MAC Address
 - Port Management
 - High Speed Flow Control
 - Software Download
 - Configuration File
 - Console/Comm Port

Configuration > Port Management

Port Management Setting

Unit **1** 2

Port	Alias	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
25	GBIC-XD (unit 1)	1	Enabled	Up	On	Disabled	1000Mbs/ Full
26			Enabled	Down	On	Disabled	1000Mbs/ Full
Switch			Enable	On	Enable		
Stack			Enable	On	Enable		

Unit **1** 2

Submit

[Ports 1 - 12](#) [Ports 13 - 24](#)

- 4 Configure the Call Server ELAN network interface on switch 2 (and 4) as show in Figure 31.

Figure 31
Call Server ELAN port configuration

Configuration > Port Management

Port Management Setting

Unit 1 2

Port	Alias	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
13			Enabled	Down	On	Enabled	
14			Enabled	Down	On	Enabled	
15			Enabled	Down	On	Enabled	
16			Enabled	Down	On	Enabled	
17			Enabled	Down	On	Enabled	
18			Enabled	Down	On	Enabled	
19			Enabled	Down	On	Enabled	
20			Enabled	Down	On	Enabled	
21			Enabled	Down	On	Enabled	
22			Enabled	Down	On	Enabled	
23			Enabled	Down	On	Enabled	
24	CS ELAN 1		Enabled	Up	On	Disabled	100Mbps / Full
Switch			Enable	On	Enable		
Stack			Enable	On	Enable		

Unit 1 2

Submit

- 5 Configure the GBIC network interface for switch 2 (and 4) as shown in Figure 32.

Figure 32
GBIC port (2) configuration

The screenshot shows the Nortel Networks Configuration > Port Management interface. On the left is a navigation menu with the following items: Access (RW), Summary, Configuration, IP, System, Remote Access, SNMPv1, SNMPv3, SNMP Trap, MAC Address Table, Find MAC Address, Port Management (selected), High Speed Flow Control, Software Download, Configuration File, and Console/Comm Port. The main content area is titled "Configuration > Port Management" and contains a "Port Management Setting" section. This section has a "Unit" selector with "1" and "2" (selected). Below this is a table with columns: Port, Alias, Trunk, Status, Link, Link Trap, Autonegotiation, and Speed / Duplex. The table has three rows: Port 25 (Alias: GBIC-XD (unit 2), Trunk: 1, Status: Enabled, Link: Up, Link Trap: On, Autonegotiation: Disabled, Speed / Duplex: 1000Mbps/ Full), Port 26 (Alias: , Trunk: , Status: Enabled, Link: Down, Link Trap: On, Autonegotiation: Disabled, Speed / Duplex: 1000Mbps/ Full), and a Switch/Stack section (Status: Enable, Link: On, Link Trap: On, Autonegotiation: Enable, Speed / Duplex:). Below the table is a "Submit" button and two links: "Ports 1 - 12" and "Ports 13 - 24".

Configuration > Port Management

Port Management Setting

Unit 1 2

Port	Alias	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
25	GBIC-XD (unit 2)	1	Enabled	Up	On	Disabled	1000Mbps/ Full
26			Enabled	Down	On	Disabled	1000Mbps/ Full
Switch			Enable	On	On	Enable	
Stack			Enable	On	On	Enable	

Unit 1 2

[Submit](#)

[Ports 1 - 12](#) [Ports 13 - 24](#)

- 6 From the main menu, choose **Application > VLAN > VLAN Configuration**.
- 7 Configure the VLANs as shown in Figure 33.

Figure 33
VLAN configuration

NORTEL NETWORKS

Access (RW)

- Configuration
- Fault
- Statistics
- Application
 - Port Mirroring
 - Rate Limiting
 - EAPOL Security
 - MAC Address Security
 - IGMP
 - VLAN
 - VLAN Configuration
 - Port Configuration
 - Port Information
 - Spanning Tree
 - MultiLink Trunk

Application > VLAN > VLAN Configuration

VLAN Table

Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
	1	VLAN #1	Port	None	0x0	IVL	Active
	2	HSP	Port	None	0x0	IVL	Active
	3	ELAN	Port	None	0x0	IVL	Active

VLAN Creation

VLAN Type:

Create VLAN

VLAN Setting

Management VLAN:

Submit

AutoPVID Setting

AutoPVID:

- 8 From the main menu, choose **Application > VLAN > Port Configuration**.
- 9 Configure the VLAN for HSP on switch 1 (and 3) as shown in Figure 34.

Figure 34
HSP VLAN configuration

Application > VLAN > Port Configuration

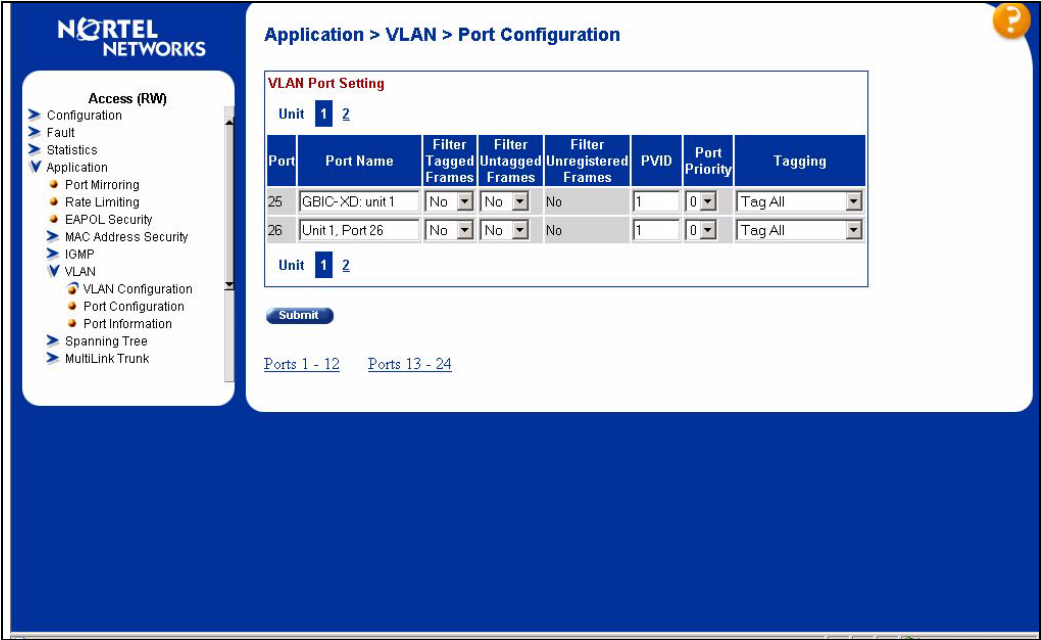
VLAN Port Setting

Unit **1** 2

Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
1	HSP-side1	No	No	No	2	0	Untag All
2	Unit 1, Port 2	No	No	No	3	0	Untag All
3	Unit 1, Port 3	No	No	No	3	0	Untag All
4	Unit 1, Port 4	No	No	No	3	0	Untag All
5	Unit 1, Port 5	No	No	No	3	0	Untag All
6	Unit 1, Port 6	No	No	No	3	0	Untag All
7	Unit 1, Port 7	No	No	No	3	0	Untag All
8	Unit 1, Port 8	No	No	No	3	0	Untag All

- 10
- Configure the GBIC VLAN network interfaces for switch 1 (and 3) as shown in Figure 35.

Figure 35
GBIC (1) VLAN configuration



- 11 Configure Call Server ELAN VLAN network interface on switch 2 (and 4) as shown in Figure 36.

Figure 36
Call Server ELAN VLAN configuration

NORTEL NETWORKS

Access (RW)

- Configuration
- Fault
- Statistics
- Application
 - Port Mirroring
 - Rate Limiting
 - EAPOL Security
 - MAC Address Security
 - IGMP
 - VLAN**
 - VLAN Configuration
 - Port Configuration**
 - Port Information
 - Spanning Tree
 - MultiLink Trunk

Application > VLAN > Port Configuration

VLAN Port Setting

Unit 1 2

Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
13	Unit 2, Port 13	No	No	No	3	0	Untag All
14	Unit 2, Port 14	No	No	No	3	0	Untag All
15	Unit 2, Port 15	No	No	No	3	0	Untag All
16	Unit 2, Port 16	No	No	No	3	0	Untag All
17	Unit 2, Port 17	No	No	No	3	0	Untag All
18	Unit 2, Port 18	No	No	No	3	0	Untag All
19	Unit 2, Port 19	No	No	No	3	0	Untag All
20	Unit 2, Port 20	No	No	No	3	0	Untag All
21	Unit 2, Port 21	No	No	No	3	0	Untag All
22	Unit 2, Port 22	No	No	No	3	0	Untag All
23	Unit 2, Port 23	No	No	No	3	0	Untag All
24	CS ELAN 1	No	No	No	3	0	Untag All

Unit 1 2

Submit

- 12 Configure the GBIC VLAN network interface for switch 2 (and 4) in the stack as shown in Figure 37.

Figure 37
GBIC (2) VLAN configuration

Application > VLAN > Port Configuration

VLAN Port Setting

Unit **1** **2**

Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
25	GBIC-XD: unit 2	No	No	No	1	0	Tag All
26	Unit 2, Port 26	No	No	No	1	0	Tag All

Unit **1** **2**

Submit

[Ports 1 - 12](#) [Ports 13 - 24](#)

- 13 From the main menu choose **Application > VLAN > VLAN Configuration**.

The **VLAN Configuration** web page opens (see Figure 33 on [page 166](#)).

- 14 Under **VLAN Creation**, in the **VLAN Type** drop-down list, choose **Port**.
- 15 Click **Create VLAN**.

The **VLAN Configuration: Port Based** web page appears.

16 Configure default VLAN port membership as shown in Figure 38.**Figure 38**
VLAN port membership configuration

NORTEL NETWORKS

Access (RW)

- > Configuration
- > Fault
- > Statistics
- > Application
 - Port Mirroring
 - Rate Limiting
 - EAPOL Security
 - > MAC Address Security
 - > IGMP
 - > **VLAN**
 - VLAN Configuration
 - Port Configuration
 - Port Information
 - > Spanning Tree
 - > MultiLink Trunk

Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN: 1

VLAN Name: VLAN #1

Learning Constraint: VL

Port	All	Port Membership																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unit 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

17 Configure HSP VLAN port membership as shown in Figure 39.

Figure 39
HSP VLAN port membership configuration

NORTEL
NETWORKS

Access (RW)

> Configuration

> Fault

> Statistics

> Application

> Port Mirroring

> Rate Limiting

> EAPOL Security

> MAC Address Security

> IGMP

> VLAN

> VLAN Configuration

> Port Configuration

> Port Information

> Spanning Tree

> MultiLink Trunk

Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN

2

VLAN Name

HSP

Learning Constraint

V/L

Port Membership

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unit 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Submit

Back

18 Configure ELAN VLAN port membership as shown in Figure 40.

Figure 40
ELAN VLAN port membership configuration

NORTEL NETWORKS

Access (RW)

- > Configuration
- > Fault
- > Statistics
- > Application
 - Port Mirroring
 - Rate Limiting
 - EAPOL Security
 - > MAC Address Security
 - > IGMP
 - > **VLAN**
 - VLAN Configuration
 - Port Configuration
 - Port Information
 - > Spanning Tree
 - > MultiLink Trunk

Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN: 3

VLAN Name: ELAN


Learning Constraint: VL

Port	All	Port Membership																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unit 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Submit **Back**

- 19 From the main menu, choose **Application > MultiLink Trunk > Group**. Configure the MultiLink Trunk Group settings as shown in Figure 41.

Figure 41
MultiLink Trunk Group settings configuration



Access (RW)

- ▼ Application
 - Port Mirroring
 - Rate Limiting
 - EAPOL Security
 - MAC Address Security
 - IGMP
 - VLAN
 - Spanning Tree
 - ▼ MultiLink Trunk
 - Group
 - Utilization
 - QoS
 - COPS
- ▼ Administration
 - System Information

Application > MultiLink Trunk > Group

MultiLink Trunk Group Setting

Trunk	Trunk Members	STP Learning	Trunk Mode	Trunk Name	Trunk Status
1	Unit: 1 2 Port: 25 25	Fast	Basic	GE100Base-3	Enabled
2	Unit: Port:	Normal	Basic	Trunk #2	Disabled
3	Unit: Port:	Normal	Basic	Trunk #3	Disabled
4	Unit: Port:	Normal	Basic	Trunk #4	Disabled
5	Unit: Port:	Normal	Basic	Trunk #5	Disabled
6	Unit: Port:	Normal	Basic	Trunk #6	Disabled

End of Procedure

Appendix B: Controlled Load-sharing zones

Contents

This section contains information on the following topics:

Network bandwidth management zones	175
Configuring zone parameters at the backup site	178
Configuring zone parameters at the home site	186
Configuring zone-based digit manipulation	193

Network bandwidth management zones

An IP Peer network is divided into different bandwidth management zones, to which each IP Phone in the network is assigned. IP Phones in the same bandwidth management zone:

- share the same IP bandwidth management policies
- are geographically near each other
- are all in the same time zone
- are all in the same PSTN dialing plan

Each IP Phone is assigned to a zone during configuration. For dialing plan purposes, IP Phones in the same zone are treated identically.

Bandwidth management zones enable IP Phones that are located in separate geographic locations to have dialing plan behaviors that are localized to the telephone location rather than the Call Server location.

With the Controlled Load-sharing configuration, the backup system must be configured with one zone for its local IP Phones and with a second zone for the redundant IP Phones (multiple zones can also be configured for a system, to take account of, for example, different floors of a building). This allows the administrator to define a different numbering plan on the backup system for the home site IP Phones for local, long distance (optional), and emergency services calls. It also allows the administrator to configure the appropriate time display for the home site IP Phones when they are in a different time zone than the backup site.

When the home site IP Phones are registered on the backup system, zone configuration data enables the backup Call Server to modify the dialed digits for calls initiated from a home site telephone. The NRS then provides the endpoint information to route the call to the appropriate destination.

Note: Throughout this document, the term “zone” is defined as a bandwidth management zone, not an NRS zone.

Zone-based digit manipulation

Zone-based digit manipulation allows the Controlled Load-sharing configuration to provide users with seamless transition when system control is passed to the backup system following home system failure. Users can continue dialing local public numbers as normal even if system control has switched to a different NPA area.

To achieve this, the Zone Access Code Behavior (ZACB) and Zone Digit Prefix (ZDP) properties must be configured on the backup system for the redundant IP Phones. ZACB and ZDP are used to add digits to the digits dialed on the home site IP Phone. The resulting digit string is then used to route the call. The net effect is that redundant IP Phone users can continue to enter the same dialed digits and be routed appropriately under control of the backup system.

For example, if “1 87654321” is dialed, where “1” is the Access Code, then:

- when the IP Phone is registered at the home system, the call is routed based on the dialed digits.
- when the IP Phone is registered at the backup system, the digits undergo zone-based digit manipulation (such as inserting “101”), and the call is routed based on the new manipulated digit string (in this example “1 101 87654321”).

Note: Special considerations apply in the case where a single Access Code is used for both on-net and off-net calls, especially when UDP is used. Routing of on-net and off-net calls is normally different. The Call Server ESN Special Number provisioning and Gatekeeper Numbering Plan Entry provisioning should be used to provide this different routing.

In the case where a single Access Code is not shared, that is, where one Access Code is exclusively used for UDP on-net dialing, standard procedures should be used. Refer to *Dialing Plans: Description* (553-3001-183).

For a given home system, more than one zone can be defined at the backup system. Therefore, different home site IP Phones can receive different routing treatments at the backup site. The combination of zone-based digit manipulation and routing capabilities can be used to achieve many other routing outcomes for home site IP Phone calls at the backup system.

Zone configuration considerations

Do not configure Zone 0, the default zone, as a home or backup system zone. Network Bandwidth Management does not support zone 0. If zone 0 is configured as a system zone, the Bandwidth Management feature is not activated.

In the home and backup systems, configure available bandwidth and preferred strategy for a zone with LD 117 or Element Manager.

This section describes the configuration of zones on the backup system for the redundant home site IP Phones.

For more information on system configuration, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213). Also refer to *Communication Server 1000E: Installation and Configuration* (553-3041-210) or *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210) as appropriate for the system.

To configure the zones at the home and backup system, perform the procedures in the following sections:

- 1 “Configuring zone parameters at the backup site” on page 178
- 2 “Configuring zone parameters at the home site” on page 186
- 3 “Configuring zone-based digit manipulation” on page 193

Configuring zone parameters at the backup site

This section describes how to configure zone parameters on the backup system to take into account the redundant home system IP Phones. The procedure is similar to an IP Peer Network configuration. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

Zone parameters are defined at the backup system in LD 117 (Procedure 17 on [page 187](#)). Time adjustments for zones are configured in LD 117 and defined relative to the time set in LD 2.

Note: The time adjustment for the zone is required only on the backup system, to account for home IP Phones that are registered from a different time zone.

Procedure 16 Configuring ESN and redundant IP Phone zones



WARNING

Before *and* after an upgrade, perform a data dump (using LD 43 EDD or through Element Manager) on the Call Server to back up the existing data.

- 1 On the backup system, Configure the Home Location Code (HLOC), and the Virtual Private Network Identifier (VPNI).

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier

Prompt	Response	Description
REQ:	CHG	Change existing data block.
TYPE:	NET	ISDN and ESN Networking options
CUST		Customer number
	0-99	Range for CS 1000M Large Systems and CS 1000E systems
...		
CLID	YES	Allow Calling Line Identification option
- ENTRY	xx	CLID entry to be configured
- - HLOC	100-9999999	Home location code (ESN) (3-7 digits)
ISDN	YES	Integrated Services Digital Network
- VPNI	(0)-16283	Virtual Private Network Identifier for Bandwidth Management Feature 0 or X = Disable feature 1-16383 = Enable feature <cr> = No Change

- 2 Configure Vacant Number Routing (VNR).

VNR must be configured to ensure the necessary routing in the case of split-registration due to network connectivity failure.

VNR is routed through the Virtual Trunk. This enables the NRS to centralize Numbering Plan definitions. To configure VNR, configure a Route List Index (RLI) with the Digit Manipulation Index (DMI) in LD 86 set to 0 (no digit manipulation required) on the Virtual Trunk route.

LD 15 – Configure Vacant Number Routing

Prompt	Response	Description
REQ:	NEW CHG	Add new data or change existing data
TYPE:	NET	Configure networking
VNR	YES	Vacant Number Routing
- RLI	0-999	Route List Index as defined in LD 86
- FLEN	1-(16)	Flexible length of digits expected
- CDPL	1-(10)	Flexible length of VNR CDP
- UDPL	1-(19)	Flexible length of VNR LOC

- On the backup system, create the home site zone.

Configure the zone properties for IP telephony bandwidth management. Use LD 117 or Element Manager. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

Note: The home system zone number and zone bandwidth management parameters at the backup system must match the corresponding home system zone number and zone bandwidth management parameters at the home system.

IMPORTANT!

Zone 0, the default zone, must not be configured as a system zone. Network Bandwidth Management does not support Zone 0. If Zone 0 is configured as a system zone, the Bandwidth Management feature is not activated.

LD 117 – Define zone properties on the backup system for the home site IP Phones (Part 1 of 2)

Command	Description
NEW ZONE <xxx> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType>]	<p>Create a new zone with the following parameters:</p> <ul style="list-style-type: none"> • xxx = 0-255 zone number • intraZoneBandwidth = Intrazone available bandwidth (see Note 1 on page 183) 0-1 000 000 Kbit/s • intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) (see Note 2 on page 183) • interZoneBandwidth = Interzone available bandwidth (see Note 1 on page 183) 0-1 000 000 Kbit/s • interZoneStrategy = Interzone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) (see Note 2 on page 183) • zoneResourceType = zone resource type (shared or private), where <ul style="list-style-type: none"> — shared = Current default zone type. The IP Phones configured in shared zones use DSP resources configured in shared zones. If all of the shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked. The order of channel selection for the gateway channels is: <ol style="list-style-type: none"> 1. channel from same zone as IP Phone is configured 2. any available channel from the shared zones channels — private = DSP channels configured in a private zone are used only by IP Phones that are also configured for that private zone. If more DSP resources than are available in the zone are required by these IP Phones, DSPs from other zones are used. However, IP Phones configured in shared zones cannot use the private zones' channels. The order of selection for the gateway channels is: <ol style="list-style-type: none"> 1. channel from same private zone as IP Phone is configured 2. any available channel from the pool of shared zones' channels

LD 117 – Define zone properties on the backup system for the home site IP Phones (Part 2 of 2)

Command	Description
<p>Note 1: If the Network Bandwidth Management feature is going to be used, the intraZoneBandwidth and interZoneBandwidth parameters must be set to the actual available bandwidth.</p> <p>Note 2: If the Network Bandwidth Management feature is going to be used, and the zone is going to be associated with a Virtual Trunk, the intraZoneStrategy and interZoneStrategy parameters must be set to BQ.</p>	

- 4 Define the zone parameters on the backup system for the redundant IP Phone zone. Use LD 117 or Element Manager. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

LD 117 – Define zone parameters on the backup system for the home site IP Phones

Command	Description
CHG ZBRN <Zone> <yes no>	Define a zone as a home system zone.
CHG ZDST <Zone> <yes no> <StartMonth> <StartWeek> <StartDay> <StartHour> <EndMonth> <EndWeek> <EndDay> <EndHour>	If the home system observes Daylight Savings Time (DST), these parameters specify the start and end of DST. During DST, the clock automatically advances one hour forward.
CHG ZTDF <Zone> <TimeDifferencefromBackupSystem>	Specified in minutes, the time difference between the backup system and the home system when each is in a different time zone.
CHG ZDES <Zone> <ZoneDescription>	A name to render data display more meaningful.

- 5 Enable the features for the home site zone in LD 117.

LD 117 – Enable features on the backup system for home site zone

Command	Description
ENL ZBR <zone> ALL	Enables features for home system <zone>.

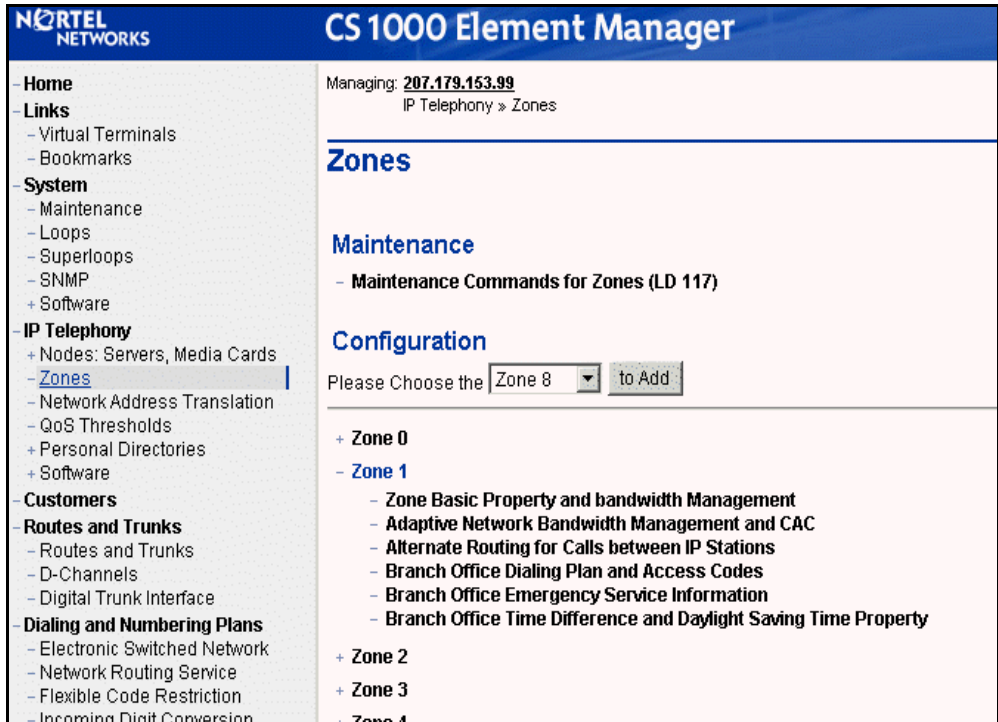
End of Procedure

Element Manager zone configuration

From Element Manager, configure the home system-specific zone properties and time difference on the backup system.

The **Zones** window (see Figure 42 on [page 185](#)) is the main window used for zone configuration in Element Manager. Select **IP Telephony > Zones** from the Element Manager navigator to open this window.

Figure 42
Zone configuration on the backup system



In the **Zone List** window, select the zone to be configured. The following properties can be configured:

- Basic Property and Bandwidth Management (see Figure 43 on [page 186](#))
- Adaptive Network Bandwidth Management and CAC
- Alternate Routing for Calls between IP Stations
- Branch Office Dialing Plan and Access Codes
- Branch Office Emergency Service Information
- Branch Office Time Difference and Daylight Saving Time Property

Figure 43
Zone Basic Property and Bandwidth Management

NORTEL
NETWORKS

CS 1000 Element Manager

Managing: **207.179.153.99**
IP Telephony » Zones » Zone 0 » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	<input type="text" value="0"/>
Intrazone Bandwidth (INTRA_BW):	<input type="text" value="100000"/>
Intrazone Strategy (INTRA_STGY):	<input type="text" value="Best Quality (BQ)"/>
Interzone Bandwidth (INTER_BW):	<input type="text" value="10000"/>
Interzone Strategy (INTER_STGY):	<input type="text" value="Best Quality (BQ)"/>
Resource Type (RES_TYPE):	<input type="text" value="Shared (SHARED)"/>
Branch Office Support (ZBRN):	<input type="text" value="MO (MO)"/>
Description (ZDES):	<input type="text" value="Zone - 00010"/>

————— End of Procedure —————

Configuring zone parameters at the home site

This section describes how to configure zone parameters on the home system to take into account the redundant IP Phones. The zones must be configured to match the zones configured on the backup system. The zones are defined in LD 117.

Procedure 17

Configuring the home system zone



WARNING

Before *and* after an upgrade, perform a data dump (using LD 43 EDD or NRS Manager) on the Call Server to back up the existing data.

- 1 Set the current date and time. See *Software Input/Output: Administration* (553-3001-311).

LD 2 – Define system date

Command	Description
STAD dd mm yyyy hh mm ss	Set the time and date: STAD DAY MONTH YEAR HOUR MINUTE SECOND

- 2 Configure the Home Location Code (HLOC) and Virtual Private Network Identifier (VPNI).

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data
TYPE:	NET	ISDN and ESN Networking options
CUST	0-99	Customer number Range for CS 1000M systems and CS 1000E systems
...		
CLID	YES	Allow Calling Line Identification Option
- ENTRY	xx	CLID entry to be configured

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier. (Part 2 of 2)

Prompt	Response	Description
-- HLOC	100-9999999	Home location code (ESN) (3-7 digits)
ISDN	YES	Integrated Services Digital Network
- VPNI	(0)-16283	Virtual Private Network Identifier for Bandwidth Management Feature 0 or X = disables feature 1-16383 = enables feature <cr> = no change

3 Configure VNR.

VNR must be configured to ensure the necessary routing in the case of split-registration due to network connectivity failure.

VNR is routed through the Virtual Trunk. This enables the NRS to centralize Numbering Plan definitions. To configure VNR, configure a RLI with the DMI in LD 86 set to 0 (no digit manipulation required) on the Virtual Trunk route.

LD 15 – Configure Vacant Number Routing

Prompt	Response	Description
REQ:	NEW CHG	Add new data or change existing data
TYPE:	NET	Configure networking
VNR	YES	Vacant Number Routing
- RLI	0-999	Route List Index as defined in LD 86
- FLEN	1-(16)	Flexible length of digits expected
- CDPL	1-(10)	Flexible length of VNR CDP
- UDPL	1-(19)	Flexible length of VNR LOC

- 4 Configure the zone properties for IP telephony bandwidth management. Use LD 117 or Element Manager (refer to Figure 44 on [page 192](#)). At the home system, this zone is used only for bandwidth management purposes. It does not have any associated time zone or dialing plan properties.

Note: The zone number and zone bandwidth management parameters at the home system must match the corresponding zone number and zone bandwidth management parameters at the backup system.

IMPORTANT!

Zone 0, the default zone, must not be configured as a system zone. Network Bandwidth Management does not support zone 0. If zone 0 is configured as a system zone, the Network Bandwidth Management feature will not be activated.

LD 117 – Define zone properties at the home system.

Command	Description
NEW ZONE <xxx> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType>]	<p>Create a new zone with the following parameters:</p> <ul style="list-style-type: none"> • xxx = 0-255 zone number • intraZoneBandwidth = Intrazone available bandwidth 0-1 000 000 Kbit/s • intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) • interZoneBandwidth = Interzone available bandwidth 0-1 000 000 Kbit/s • interZoneStrategy = Interzone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) • zoneResourceType = zone resource type (shared or private), where <ul style="list-style-type: none"> — shared = Current default zone type. The IP Phones configured in shared zones use DSP resources configured in shared zones. If all of the shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked. The order of channel selection for the gateway channels is: <ol style="list-style-type: none"> 1. channel from same zone as IP Phone is configured 2. any available channel from the shared zones' channels — private = DSP channels configured in a private zone are used only by IP Phones that are also configured for that private zone. If more DSP resources than are available in the zone are required by these IP Phones, DSPs from other zones are used. However, IP Phones configured in shared zones cannot use the private zones' channels. The order of selection for the gateway channels is: <ol style="list-style-type: none"> 1. channel from same private zone as IP Phone is configured 2. any available channel from the pool of shared zones' channels

End of Procedure

Element Manager zone configuration on the home system

Figure 44 shows the only zone configuration screen required on the home system. It is an alternative to zone configuration using LD 117.

Figure 44
Zone Basic Property and Bandwidth Management

The screenshot displays the Nortel CS 1000 Element Manager web interface. The left sidebar contains a navigation menu with categories: Home, Links, System, IP Telephony, Customers, Routes and Trunks, and Dialing and Numbering Plans. The 'IP Telephony' section is expanded, showing 'Zones' as the selected option. The main content area is titled 'Zone Basic Property and Bandwidth Management'. At the top, it shows the IP address '207.179.153.99' and the breadcrumb 'IP Telephony » Zones » Zone 0 » Zone Basic Property and Bandwidth Management'. Below the title, there is a table with two columns: 'Input Description' and 'Input Value'. The table contains the following entries:

Input Description	Input Value
Zone Number (ZONE):	0
Intrazone Bandwidth (INTRA_BW):	100000
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	10000
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Branch Office Support (ZBRN):	MO (MO)
Description (ZDES):	Zone - 00010

At the bottom of the form, there are four buttons: Submit, Refresh, Delete, and Cancel.

Add the Signaling Server name to the network NRS database using NRS Manager.

Note: If the Signaling Server name is not added to the NRS database, the NRS rejects any registration request from the Signaling Server because its name is not in the ID list. The ID is case-sensitive.

Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for the appropriate procedure.

Configuring zone-based digit manipulation

Perform the following steps to configure the dialing plan on the backup system to provide PSTN access to home site IP Phones are:

- 1 Configure the ZACB property for the home system zone.
- 2 Configure the ZDP property for the home system zone.

These steps can be done using overlays, as described in this section, or in Element Manager. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for more details.

Procedure 18

Configuring the zone-based digit manipulation

- 1 Configure the ZACB property on the backup system for the home system zone.

LD 117 – Define the zone Access Code handling for the home system zone.

Command	Description
CHG ZACB <zone> [ALL][<AC1 AC2> <AC1 AC2>]	Define the Access Codes used to modify local (or long distance) calls to force all calls local to the home site to be routed to the home site PSTN.

The ZACB and ZDP properties are used to configure the digit manipulation behavior of the home system zone.

The ZACB property specifies which calls undergo digit manipulation. The attribute can be configured in the following ways:

- CHG ZACB <zone>
In this configuration, dialing AC1 or AC2 does not trigger digit manipulation. Home system calls are treated exactly the same as those for backup system users.
- CHG ZACB <zone> ALL

In this configuration, calls dialed with AC1 and calls dialed with AC2 undergo zone-based digit manipulation.

For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If a user dials "1 87654321", ZDP is inserted in the dialed digits to form a digit string of "1 101 87654321". If a user dials "2 87654321", ZDP is inserted in the dialed digits to form a digit string of "2 101 87654321".

- CHG ZACB <zone> AC1 AC2

In this configuration, only calls dialed with AC1 undergo zone-based digit manipulation.

For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If a user dials "1 87654321", ZDP is inserted in the dialed digits to form a digit string of "1 101 87654321". If a user dials "2 87654321", zone-based digit manipulation does not occur and the digit string remains unchanged.

- CHG ZACB <zone> AC2 AC2

In this configuration, only calls dialed with AC2 undergo zone-based digit manipulation.

For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If a user dials "1 87654321", zone-based digit manipulation does not occur and the digit string remains unchanged. If a user dials "2 87654321", ZDP is inserted in the dialed digits to form a digit string of "2 101 87654321".

Note 1: As part of the ZACB configuration, the dialed Access Code can also be changed; so if AC2 is dialed, the Access Code can be changed to AC1, or vice versa. This provides more flexibility in the home system NARS configurations. Normally, there is no need to change the Access Code.

Note 2: The Access Code dialed by the user is used internally by the Call Server. It is not sent as part of the outpulsed digits (to the NRS or to the trunks).

Note 3: If a specified Access Code is used for both local and long distance dialing, then both types of calls receive the specified routing.

- 2 Configure the ZDP property for the home system zone at the backup system. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

LD 117 – Define the zone digit manipulation on the backup system for the home site zone

Command	Description
CHG ZDP <zone> <DialingCode1> <DialingCode2> <DialingCode3>	Define the dialing plan for the home system zone, where DialingCode1, DialingCode2, and DialingCode3 are inserted into the dialed digits between the Access Code and the remainder of the dialed number.

The ZDP and ZACB (step 1 on [page 193](#)) properties are used to configure the digit manipulation behavior of the home system zone.

The ZDP property is inserted between the Access Code specified in the ZACB command and the dialed digits. This zone-based digit manipulation allows the backup system Call Server and the network NRS to distinguish the home site IP Phone calls from the backup site IP Phone calls, and route them accordingly. The digit manipulation occurs before any digit processing in the backup system Call Server or NRS.

Note: If DialingCode1, DialingCode2, or DialingCode3 are already present in the dialed digits, then they will not be re-inserted.

The Access Code (“1”) is not included in the digit string that is sent to the NRS. The NRS recognizes “101” at the front of the digit string and routes the call to the destination.

End of Procedure

Configuration example for PSTN resources

IP Phones registered on the backup system can be grouped into one of two categories:

- those physically located at the backup site and, therefore, configured with the backup site dialing plan
- those physically located at the home site and, therefore, configured with a dialing plan for the home site zone

Customer data must first be configured to recognize numbers that are local to each location (a standard NARS configuration issue). This example specifically focuses on the additional changes necessary to physically enable a home system telephone, registered with the backup system, to reach the PSTN at the home site.

Note: Assume that the home system and backup system have been configured with local numbers, such as 555-1212 or 967-1111.

Table 13 uses the following configuration at the backup system for home system telephones to reach the PSTN.

Table 13
Example dialing string, area codes, and Access Codes (Part 1 of 2)

	At the backup system node	At the home system node
Local dialing string	Local calls use 7-digit dialing.	Local calls use 7-digit dialing.
Area code (NPA)	The NPA is 613.	The NPA is 506.
Country code	The home system Node Country Code is 1.	The backup system Node Country Code is 1.
NARS configuration	Local calls use AC2, which is “9”. Long-distance calls use AC1, which is “6”.	Local calls use AC2, which is “9”. Long distance calls use AC1, which is “6”.

Table 13
Example dialing string, area codes, and Access Codes (Part 2 of 2)

	At the backup system node	At the home system node
The Public National (E.164) entry points to...	“506” points to home system node.	“613” points to backup system node.

At the backup system, a zone must be configured for the home site IP Phones. In the definition of the home site zone, the ZACB and ZDP properties must be configured to insert the home site NPA into the dialed digits.

If a local backup system telephone goes off-hook and dials “9 555-1212”, the Call Server assumes the user intends to reach the number 555-1212 in the local NPA. The fully-qualified number (E.164) is 1-613-555-1212.

If a home site IP Phone user goes off-hook and dials “9 555-1212” and the ZDP property is configured, the Call Server directs the user to the number 555-1212 in the NPA local to the home user. The fully-qualified number (E.164) is 1-506-555-1212.

Nortel Communication Server 1000

System Redundancy

Copyright © 2006 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, Nortel (Logo), the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Publication number: 553-3001-307

Document release: Standard 4.00

Date: July 2006

Produced in Canada

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

