



Nortel Communication Server 1000

System Redundancy Fundamentals

Document status: Standard
Document version: 01.01
Document date: 30 May 2007

Copyright © 2004-2007, Nortel Networks
All Rights Reserved.

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

All other trademarks are the property of their respective owners.

Revision history

May 2007

Standard 01.01. This document This document is renumbered and updated for Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: CS 1000: System Redundancy (553-3001-307).

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).

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.

4 Revision history

Nortel Communication Server 1000
System Redundancy Fundamentals
NN43001-507 01.01 Standard
Release 5.0 30 May 2007

Contents

New in this release	11
Features 11	
Geographic Redundancy: Survivable Media Gateway 11	
Temporary IP User license 11	
High Availability (HA) package enhancement 11	
Other changes 12	
Applicable systems 12	
Conventions 12	
Related information 12	
Online 13	
CD ROM 13	
<hr/>	
How to get help	15
Getting help from the Nortel Web site 15	
Getting help over the telephone from a Nortel Solutions Center 15	
Getting help from a specialist by using an Express Routing Code 15	
Getting help through a Nortel distributor or reseller 16	
<hr/>	
Overview	17
Contents 17	
Geographic Redundancy 17	
Survivable Media Gateway configuration 17	
Controlled Load-sharing configuration 18	
Campus Redundancy 19	
<hr/>	
Geographic Redundancy: Survivable Media Gateway configuration	21
Contents 21	
Description 22	
Software 22	
Hardware 23	
Database replication 23	
Normal operation 23	
Triple IP registration 24	
Redirection process 25	

- Automatic NUID 26
- Survival Media Gateway NRS routing examples 28
- Vacant Number Routing for TDM digital and analog telephones 30
- Active Call Failover 30
- Abnormal operation 30
 - Primary system failure 30
 - Secondary system failure 35
 - Network connectivity failure call scenarios 35
- Survivable Media Gateway planning 37
 - Common CS 1000E planning considerations 38
- Survivable Media Gateway configuration 40
- Configuring the Primary Call Server 42
 - Configure a Backup Rule (BKR) 42
 - Configure a Backup Schedule (BKPS) 45
 - GRNS command 47
 - Configure Database Replication Control (GRDRC) block 48
 - Configure SECRET string for database replication 49
 - Configure State Control (GRSC) Blocks 51
 - Configure the Media Gateway Controller (MGC) 53
 - Configure IP telephony nodes 54
 - Configure Primary (S1) and Secondary (S2) Connect Servers 55
- Adding a new Secondary Call Server to the system 55
- Secondary system ACTIVE operation 56
- Primary system recovery 57
- Upgrades 59
- Maintenance 60
 - TM 3.1 60
 - Database configuration 60
 - Manual database replication and restore 60
- Diagnostics 62
 - System status 62
- System faults 64
 - FTP transfer failure 64
 - Secondary system database endorsement failure 64
- Feature interactions 65
- System monitoring 65
 - SNMP system alarms monitoring 65

Geographic Redundancy 1+1 configuration 67

- Contents 67
- Description 67
- Upgrading an existing 1+1 configuration to Survivable Media Gateway 67

Geographic Redundancy Controlled Load-sharing configuration	71
Contents	71
Description	71
Normal operation	72
Redirection process	73
Database configuration	73
Software	74
Hardware	74
Site 1 system failure	75
Site 2 system failure	76
Planning a Controlled Load-sharing configuration	77
Additional planning considerations	78
Network Bandwidth Management	81
Numbering plan	81
Branch Office support	83
NRS Routing for Branch Office	84
Installing a Controlled Load-sharing configuration	86
Provisioning the IP Phones	87
Maintenance	88
Feature interactions	88
System monitoring	88
Campus Redundancy	89
Contents	89
Description	90
High Availability (HA) package enhancement	91
High Speed Pipe (HSP) IP address management enhancement	91
Stop and Copy protocol enhancement	91
Operating parameters	92
Normal Operations	92
Warm start and Cold start	93
Fault Detection	94
Switchover	94
Heartbeat	97
Network topology	97
Baystack 470 GBIC Fibre Interfaces	97
Campus Redundancy Baystack 470 Bandwidth Use	98
Switching Equipment	99
Call Server operation during IP network failure	100
ELAN subnet connectivity between the CPUs is lost but HSP is still operational	101

HSP connectivity is lost but ELAN subnet connectivity between the CPUs is operational	101
ELAN subnet and HSP connectivity is lost between the CPUs	101
HSP configuration	102
Initial installation	102
HSP recommendations and rules	102
High Speed Pipe IP address configuration	103
Customer validation	108
IP Telephony node configuration	108
Upgrading a redundant system	108
Downgrading a redundant system	110
HSP maintenance	111
STAT CPU	111
STAT HSP	113
STAT ELNK	114
Troubleshooting	115

Appendix A Configuring the BayStack 470-24T for Campus Redundancy **117**

Contents	117
Description	117
BayStack 470-24T configuration	119

Appendix B Controlled Load-sharing zones **127**

Contents	127
Network bandwidth management zones	127
Zone-based digit manipulation	128
Configuring zone parameters at the backup site	129
Element Manager zone configuration	134
Configuring zone parameters at the home site	135
Element Manager zone configuration on the home system	138
Configuring zone-based digit manipulation	139
Configuration example for PSTN resources	141

Procedures

Procedure 1	Configuring a Survivable Media Gateway system	40
Procedure 2	Configuring a Backup Rule in Element Manager	44
Procedure 3	Configuring a Backup Schedule in Element Manager	46
Procedure 4	Configuring GRDRC block in Element Manager	49
Procedure 5	Configuring SECRET string in Element Manager	50
Procedure 6	Configuring GRSC block in Element Manager	52
Procedure 7	Configuring the Media Gateway Controller in Element Manager	53
Procedure 8	Configuring IP telephony nodes in Element Manager	54
Procedure 9	Adding a new Secondary Call Server to the system	55
Procedure 10	Clearing secondary system ACTIVE state in Element Manager	57

Procedure 11	Recovering the primary system database	58
Procedure 12	Testing the recovered primary system	59
Procedure 13	Manual database restore in Element Manager	61
Procedure 14	Checking system status in Element Manager	63
Procedure 15	Testing Survival Media Gateway system in Element Manager	64
Procedure 16	Upgrading an existing 1+1 configuration to Survivable Media Gateway	68
Procedure 17	Installing Controlled Load-sharing configuration	86
Procedure 18	Configuring the BayStack 470-24T using Web-based management	119
Procedure 19	Configuring ESN and redundant IP Phone zones	130
Procedure 20	Configuring the home system zone	135
Procedure 21	Configuring the zone-based digit manipulation	139

New in this release

This chapter contains information on new System Redundancy features available with CS 1000 Release 5.0.

Features

CS 1000 Release 5.0 provides several new features and enhancements for geographic and system redundancy. These include:

Geographic Redundancy: Survivable Media Gateway

The Survivable Media Gateway enhancement over 1+1 configurations lets you provision up to 50 Secondary Call Servers to a Primary Call Server. A database is administered on the Primary server and replicated to all Secondary servers in the system. Redundancy is provided for both IP and TDM resources through triple IP registration, which enhances system redundancy by allowing network resources to specify up to three choices for service in the event of system or network connectivity failure.

Temporary IP User license

The Temporary IP User licensing enhancement limits the number of IP set Terminal Numbers (TN) that have the Network User ID (NUID) configured. These TNs are not included in the total number of license limitations for IP User, Basic IP User, or Automatic Call Distribution (ACD) agent usage, which makes this option more cost-effective than IP User license or Basic IP User license.

High Availability (HA) package enhancement

The Campus Redundancy enhancements in Release 5.0 include the addition of the 410 HIGH_AVAIL HIGH AVAILABILITY (HA) package for CP PM servers. If the HA package is present in the keycode, the CP PM Call Server uses the High Speed Pipe (HSP) to detect the presence of the other core. If the other core is detected, both cores negotiate to determine which is the active core and which is the standby core. If the CP PM Call Server cannot detect the other core, it starts as a single core system.

Other changes

Other changes to note for this release include:

- Rebranding of OTM 2.2 to TM 3.1

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 5.0 software. For more information about legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

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

Note: When upgrading software, you may have to upgrade memory 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 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E) CP PII, CP PIV, CP PM
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Converging the Data Network with VoIP Fundamentals (NN43001-260)*

- *Dialing Plans Reference (NN43001-283)*
- *Signaling Server Installation and Commissioning (NN43001-312)*
- *IP Peer Networking Installation and Commissioning (NN43001-313)*
- *Branch Office Installation and Commissioning (NN43001-314)*
- *Features and Services Fundamentals (NN43001-106)*
- *Software Input/Output Administration (NN43001-611)*
- *IP Line: Description, Installation, and Operation (NN43100-500)*
- *Software Input/Output Reference Maintenance (NN43001-711)*
- *Communication Server 1000M and Meridian 1 Small System Planning and Engineering (NN43021-220)*
- *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning (NN43021-310)*
- *Communication Server 1000E Planning and Engineering (NN43041-220)*
- *Communication Server 1000E Installation and Commissioning (NN43041-310)*
- *Security Management Fundamentals (NN43001-604)*

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.

How to get help

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

Getting help from the Nortel Web site

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

www.nortel.com/support

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

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

Getting help over the telephone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Overview

Contents

This section contains information about the following topics:

- "Geographic Redundancy" (page 17)
 - "Survivable Media Gateway configuration" (page 17)
 - "Controlled Load-sharing configuration" (page 18)
- "Campus Redundancy" (page 19)

Geographic Redundancy

CS 1000M systems (CP PII, CP PIV) and CS 1000E (CP PII, CP PIV, CP PM) systems provide core redundancy using dual processors so that a system remains operational following a local component failure.

Geographic Redundancy further increases the reliability of CS 1000M Systems (CP PII, CP PIV) and CS 1000E (CP PII, CP PIV, CP PM) systems by providing a remote system to serve as a backup for a local system. Depending on the configuration, the remote backup system ensures continued service for resources in case of a catastrophic failure (for example, as a result of floods or fire).

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

The main types of Geographic Redundancy configurations are as follows:

- "Survivable Media Gateway configuration" (page 17)
- "Controlled Load-sharing configuration" (page 18)

Survivable Media Gateway configuration

Communication Server Release 5.0 introduces Survivable Media Gateway as an enhancement over the existing Geographic Redundancy: 1+1 configuration. The Survivable Media Gateway configuration consists of one Primary Call Server and up to 50 Secondary Call Servers. Survivable Media Gateway redundancy provides Primary Call Server redundancy,

Wide Area Network (WAN) failure redundancy, and both IP and TDM resources redundancy. You can implement the Survivable Media Gateway configuration using any combination of CS 1000E (CP PIV, CP PM) systems.

Two software packages support the Survivable Media Gateway 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 across the Wide Area Network (WAN).

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

For more information about Survivable Media Gateway configuration, see ["Geographic Redundancy: Survivable Media Gateway configuration"](#) (page 21).

1+1 configuration

With the introduction of Survivable Media Gateway, Nortel no longer recommends 1+1 configurations. For more information about 1+1 configurations, see previous issues of this document.

Controlled Load-sharing configuration

The Controlled Load-sharing configuration provides additional system redundancy for IP Phones by allowing active systems in a network to provide redundancy for each other.

You can implement the Controlled Load-sharing configuration using different system types. A CS 1000M system can back up a CS 1000E system, and a CS 1000E system can back up a CS 1000M System.

The Controlled Load-sharing configuration employs similar functionality to the Branch Office feature. For more information, see Branch Office Installation and Commissioning (NN43001-314). You must configure a Directory Number (DN) and Terminal Number (TN) for each IP Phone on the 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 if the home system fails.

On the backup system, each IP Phone has an assigned 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 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.

A new licensing enhancement, the Temporary IP User license, limits the number of IP set TNs which have NUID configured. The total number of license limitations for IP User, Basic IP User, or ACD agent usage does not include these TNs, which makes this option more cost-effective than Basic IP User or IP User licenses.

For more information, see ["Geographic Redundancy Controlled Load-sharing configuration"](#) (page 71).

N+1 configuration

Nortel does not support N+1 configurations as of Communication Server Release 5.0. Existing N+1 configurations automatically convert to Controlled Load Sharing with Temporary IP User license configurations upon upgrade to Release 5.0.

For more information about N+1 configuration, refer to previous issues of this document.

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 and allows the remote standby Call Server to assume system control if the active Call Server fails.

Note: CS 1000M systems do not support Campus Redundancy.

You can use the Campus Redundancy feature to separate the CS 1000E Call Servers in a campus environment and enable two Call Servers, one active and one redundant, to connect through an Ethernet network interface. Campus Redundancy operates using a number of Layer 2 switching products, including the BayStack 470.

To separate the redundant Call Servers, the ELAN and HSP subnets can be extended between the two processors with Ethernet switches using Layer 2 protocol.

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

For more information about Campus Redundancy, see "[Campus Redundancy](#)" (page 19).

Geographic Redundancy: Survivable Media Gateway configuration

Contents

This section contains information about the following topics:

- "Description" (page 22)
- "Normal operation" (page 23)
 - "Triple IP registration" (page 24)
 - "Redirection process" (page 25)
 - "Automatic NUID" (page 26)
 - "Survival Media Gateway NRS routing examples" (page 28)
 - "SNMP system alarms monitoring" (page 65)
 - "Vacant Number Routing for TDM digital and analog telephones" (page 30)
 - "Active Call Failover" (page 30)
- "Abnormal operation" (page 30)
 - "Primary system failure" (page 30)
 - "Secondary system operating states" (page 31)
 - "OUTOFLICENSE state" (page 34)
 - "Secondary system failure" (page 35)
 - "Network connectivity failure call scenarios" (page 35)
- "Survivable Media Gateway planning" (page 37)
 - "Common CS 1000E planning considerations" (page 38)
- "Survivable Media Gateway configuration" (page 40)
 - "Configuring the primary system" (page 42)
 - "Adding a new Secondary Call Server to the system" (page 55)
 - "Secondary system ACTIVE operation" (page 56)
 - "Primary system recovery" (page 57)
- "Upgrades" (page 59)

- ["Maintenance" \(page 60\)](#)
- ["Diagnostics" \(page 62\)](#)
 - ["System status" \(page 62\)](#)
 - ["System faults" \(page 64\)](#)
- ["Feature interactions" \(page 65\)](#)
- ["System monitoring" \(page 65\)](#)

Description

Geographic Redundancy: Survivable Media Gateway enhances the reliability of CS 1000E systems by allowing the provisioning of up to 50 geographically remote Secondary Call Servers to a Primary Call Server. You can configure each Secondary Call Server as Alternate Call Server 1 or Alternate Call Server 2 for the devices assigned to it.

Survivable Media Gateway provides two levels of redundancy. If the Primary Call Server fails, local and remote resources register with the Secondary Call Server configured as Alternate Call Server 1. If the WAN fails, local resources register with the Secondary Call Server configured as Alternate Call Server 2.

In addition to the redundancy provided for IP resources, Survivable Media Gateway provides redundancy for TDM resources through triple IP registration. Devices register to the Primary Call Server as first choice, Alternate Call Server 1 as second choice, and Alternate Call Server 2 as third choice. For more information about triple IP registration, see ["Triple IP registration" \(page 24\)](#).

The Primary Call Server administers the database and replicates it to the Secondary Call Servers manually or by automatic scheduling. For more information about database replication, see ["Database replication" \(page 23\)](#).

You can implement the Survivable Media Gateway configuration using different system types. The Primary and Secondary Call Servers can be any combination of CS 1000E (CP PIV, CP PM) systems.

Software

Geographic Redundancy: Survivable Media Gateway is supported only in Communication Server Release 5.0 and later. This software must be installed on the Primary Call Server and all Secondary Call Servers in the system.

Hardware

Survivable Media Gateway makes use of the triple IP registration feature available in Release 5.0 for the following devices:

- Media Gateway 1000E (with new Media Gateway Controller [MGC] that replaces the SSC)
- ITG-SA
- Media Card 32S
- MGC DSP Daughterboards

For more information about triple IP registration, see ["Triple IP registration" \(page 24\)](#).

Database replication

In a Geographic Redundancy: Survivable Media Gateway configuration, you can configure and modify the database on the Primary Call Server and replicate it to all Secondary Call Servers. You can initiate manual or scheduled database replication.

For more information about manual database replication, see ["Manual database replication and restore" \(page 60\)](#). For more information about scheduled database replication, see ["Configure Database Replication Control Block \(GRDRC\) " \(page 48\)](#).

To increase the security of database replication, the zipped database is encrypted on the Primary Call Server using a SECRET string before it is replicated to the Secondary Call Servers. On each Secondary Call Server, the zipped file is decrypted using the same SECRET string. If the decryption fails, the database is not restored. The SECRET string is not replicated with the database so it must be configured separately on each Call Server in the system.

For more information about the SECRET string, see ["Configure SECRET string for database replication" \(page 49\)](#).

Normal operation

A Geographic Redundancy: Survivable Media Gateway configuration consists of the following components:

- one Primary Call Server
- up to 50 Secondary Call Servers

In a Survivable Media Gateway configuration, the Primary Call Server registers all of the system resources but has no peripheral equipment directly connected to it. The Primary Call Server serves only the peripheral

equipment connected to the Secondary Call Servers. You can configure each Secondary Call Server in the system as an Alternate Call Server 1 (AC1) or an Alternate Call Server 2 (AC2) for all or part of the system resources.

Note: Nortel recommends that you configure a Secondary Call Server as Alternate Call Server 2 in the same local area as the assigned resources. This helps to provide redundancy in the event of WAN failure.

Music, Recorded Announcement (RAN), Conference, and local trunk resources are allocated to the same zone as the user.

You can implement the Survivable Media Gateway configuration using different system types. The Primary and Secondary Call Servers can be any combination of CS 1000E (CP PIV, CP PM) systems.

Table 1 "Survivable Media Gateway supported CPU types" (page 24) shows a list of supported Call Servers.

Table 1
Survivable Media Gateway supported CPU types

		Primary Call Server CPU Type	
		CP PIV	CP PM
Secondary Call Server CPU Type	CP PIV	Yes	Yes
	CP PM	Yes	Yes

Triple IP registration

Survivability over Layer 3 network connections for TDM resources is established by triple IP registration. Therefore, you can configure a device with first, second, and third choice preferences for Call Server IP addresses.

The following devices support triple IP registration:

- Media Gateway 1000E (with the new Media Gateway Controller that replaces the SSC)
- ITG-SA
- Media Card 32S
- MGC DSP Daughterboards

Note: ITG-SA and Media Card 32S support triple IP registration for voice Media Gateway applications only.

Under normal operating conditions, all devices are registered to the Primary Call Server. If the Primary Call Server fails, the device registers to the assigned Alternate Call Server 1. If a WAN fails, the device registers to the assigned Alternate Call Server 2.

A device that loses connection to its Primary Call Server first attempts to connect to the Primary Call Server using an alternative connection as provided by the Dual Homing feature. If the connection attempt fails, it registers to the assigned Alternate Call Server 1, even if the Primary Call Server remains active. If a device cannot connect to the Alternate Call Server 1, it registers with the assigned Alternate Call Server 2.

The Media Gateway Controller is registered to the same Call Server as the Media Cards associated with the MGC. When a Media Gateway (MG) 1000E registers to a Call Server, the Call Server sends a message to all the Media Cards on that MG 1000E to register to it.

ITG-SA, Media Card 32S, and MGC DSP Daughterboards are configured on the Primary Call Server. The Primary Call Server replicates these settings to the Secondary Call Servers during database replication.

Media Gateway Controllers are configured on the Primary Call Server using Element Manager or through the command line interface of the Media Gateway Controller. For information about configuring the Media Gateway Controller, see *Communication Server 1000E Installation and Commissioning (NN43041-310)*.

Redirection process

In the Survivable Media Gateway configuration, all IP Phones in the system are configured with their Primary Connect Server (S1) pointing to the local secondary node Terminal Proxy Server (TPS) and their Secondary Connect Server (S2) pointing to the primary system node TPS.

When the IP Phones are reset, they attempt to register with the secondary. The secondary accepts these registration requests and automatically redirects all IP Phones to the primary system for registration.

Registration scenarios

IP Phones remain registered on the secondary only if the redirection process fails due to a failure at the Primary site or as a result of network connectivity failure. The following examples describe possible registration scenarios:

Scenario 1 An IP Phone can register on the Primary Call Server, Alternate Call Server 1, or Alternate Call Server 2.

- If the primary system is active, the IP Phone registers on the primary system (as pointed to by S2).

- If the Alternate Call Server 1 is active, the IP Phone registers on the Alternate Call Server 1.
- Otherwise, the IP Phone remains registered on the Alternate Call Server 2 (as pointed to by S1).

Scenario 2 An IP Phone can register on the Primary Call Server or Alternate Call Server 1.

- If the primary system is active, the IP Phone registers on the primary system (as pointed to by S2).
- Otherwise, the IP Phone remains registered on the Alternate Call Server 1 (as pointed to by S1).

Scenario 3 An IP Phone can register on the Primary Call Server or Alternate Call Server 2.

- If the primary system is active, the IP Phone registers on the primary system (as pointed to by S2).
- Otherwise, the IP Phone remains registered on the Alternate Call Server 2 (as pointed to by S1).

Automatic NUID

To redirect calls to the primary system, the secondary 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. For more information about Branch Office, see *Branch Office Installation and Commissioning (NN43001-314)*.

However, unlike the BUID in Branch Office (or the NUID in the Controlled Load-sharing configuration), the NUIDs in the Survivable Media Gateway configuration are generated automatically, rather than manually.

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

Automatic NUID = (AC1 or AC2) + HLOC + DN

[Table 2 "Logic of NUID automatic generation" \(page 26\)](#) describes in greater detail the logic used by the secondary system when it generates the NUID.

Table 2
Logic of NUID automatic generation

Variable	Logic
AC1 or AC2	In LD 15, Customer Data block, if LOC is associated with AC2, the secondary system uses AC2 to build the NUID. Otherwise, it uses AC1.

Variable	Logic
	<p>Values for AC1 or AC2 are defined in LD 86.</p> <p>(For more information, see <i>Software Input/Output Administration (NN43001-611)</i> .)</p>
HLOC	<p>The secondary system generates the NUID using the value of HLOC as defined in LD 15.</p> <p>(Configure the same HLOC in LD 90 for the appropriate AC1 or AC2. For more information, see <i>Software Input/Output Administration (NN43001-611)</i>.)</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 used to generate the NUID. If no DN meets this criteria, the NUID cannot be generated.</p> <p>Note: For the ACD 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 and copied to the secondary system during the database replication process. The NUID is created with the HLOC value originally defined on the primary system. The secondary system can use the NUID value to query the Network Redirect 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](#)" (page 81) for details.)

The following summarizes 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 TPS, and then with the secondary system.
2. The secondary system accepts the registration, and 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 Survivable Media Gateway configuration uses the NUID for redirection only. When the IP Phone registers on the primary system, the phone 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) need not be defined in LD 11 for the IP Phones in a Survivable Media Gateway configuration. For more information about NHTN, see "[Geographic Redundancy Controlled Load-sharing configuration](#)" (page 71).

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 local 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.

Survival Media Gateway NRS routing examples

Example 1

Scenario based on the following configuration:

- Primary Call Server (HLOC 343)
- 2 Alternate 2 Call Servers (SCS_DEV, SCS_VER, HLOC 343)
- 2 IP Phones configured as follows:
 - IP Phone A with DN 5000; S1 pointing to Alternate 2 Call Server (SCS_VER); S2 pointing to Primary Call Server
 - IP Phone B with DN 6000; S1 pointing to Alternate 2 Call Server (SCS_DEV); S2 pointing to Primary Call Server

The NRS routing entries are as follows:

Table 3
NRS routing entries for Example 1

UDP and CDP	Call Server
UDP 34350	cost 1 Primary Call Server
UDP 34350	cost 2 Alternate 2 Call Server (SCS_VER)
CDP 50	cost 1 Primary Call Server
CDP 50	cost 2 Alternate 2 Call Server (SCS_VER)
UDP 34360	cost 1 Primary Call Server
UDP 34360	cost 2 Alternate 2 Call Server (SCS_DEV)
CDP 60	cost 1 Primary Call Server
CDP 60	cost 2 Alternate 2 Call Server (SCS_DEV)

Example 2

Scenario based on the following configuration:

- Primary Call Server (HLOC 343)
- 2 Alternate 1 Call Servers (LSCS_DEV, LSCS_VER, HLOC 343)
- 2 Alternate 2 Call Servers (SCS_DEV, SCS_VER, HLOC 343)
- 2 IP Phones configured as follows:
 - IP Phone A with DN 5000; S1 pointing to Alternate 2 Call Server (SCS_VER); S2 pointing to Primary Call Server
 - IP Phone B with DN 6000; S1 pointing to Alternate 2 Call Server (SCS_DEV); S2 pointing to Primary Call Server

The NRS routing entries are as follows:

Table 4
NRS routing entries for Example 2

UDP and CDP	Call Server
UDP 34350	cost 1 Primary Call Server
UDP 34350	cost 2 Alternate 1 Call Server (LSCS_VER)
UDP 34350	cost 3 Alternate 2 Call Server (SCS_VER)
CDP 50	cost 1 Primary Call Server
CDP 50	cost 2 Alternate 1 Call Server (LSCS_VER)
CDP 50	cost 3 Alternate 2 Call Server (SCS_VER)
UDP 34360	cost 1 Primary Call Server

UDP and CDP	Call Server
UDP 34360	cost 2 Alternate 1 Call Server (LSCS_DEV)
UDP 34360	cost 3 Alternate 2 Call Server (SCS_DEV)
CDP 60	cost 1 Primary Call Server
CDP 60	cost 2 Alternate 1 Call Server (LSCS_DEV)
CDP 60	cost 3 Alternate 2 Call Server (SCS_DEV)

Vacant Number Routing for TDM digital and analog telephones

Vacant Number Routing (VNR) for TDM digital and analog telephones is supported with Release 5.0 and later. The TDM telephone is defined on a Media Gateway registered on one of the Secondary Call Servers in the Survivable Media Gateway configuration. TDM vacant numbers are routed to the NRS, which resolves the location of the Media Gateway where the TDM telephone is defined. VNR limitations for IP calls also apply to TDM calls.

For more information about how VNR and NRS handle calls during Primary Call Server failure or network connectivity issues, see "[Network connectivity failure call scenarios](#)" (page 35)

Active Call Failover

Active Call Failover ensures that active calls are not dropped during switchover.

For more information about Active Call Failover, see *IP Line: Description, Installation, and Operation (NN43100-500)*.

Abnormal operation

Primary system failure

In the Survivable Media Gateway 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 (N1) and Media Gateways (N2) registered on the secondary system. When the number of IP Phones (N1) or Media Gateways (N2) registered on the secondary system exceeds the Geographic Redundancy thresholds for IP Phones (GRTHR1) and Media Gateways (GRTHR2), the secondary system escalates to ACTIVATING state. (GRTHR1 and GRTHR2 are defined in LD 117.)

Secondary system operating states

The secondary system provides a number of operating states that allow smooth transition from INACTIVE to ACTIVE and back again. See [Figure 1 "Secondary system operating state logic" \(page 32\)](#) and [Table 5 "Secondary system state control data set" \(page 33\)](#) 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 1
Secondary system operating state logic

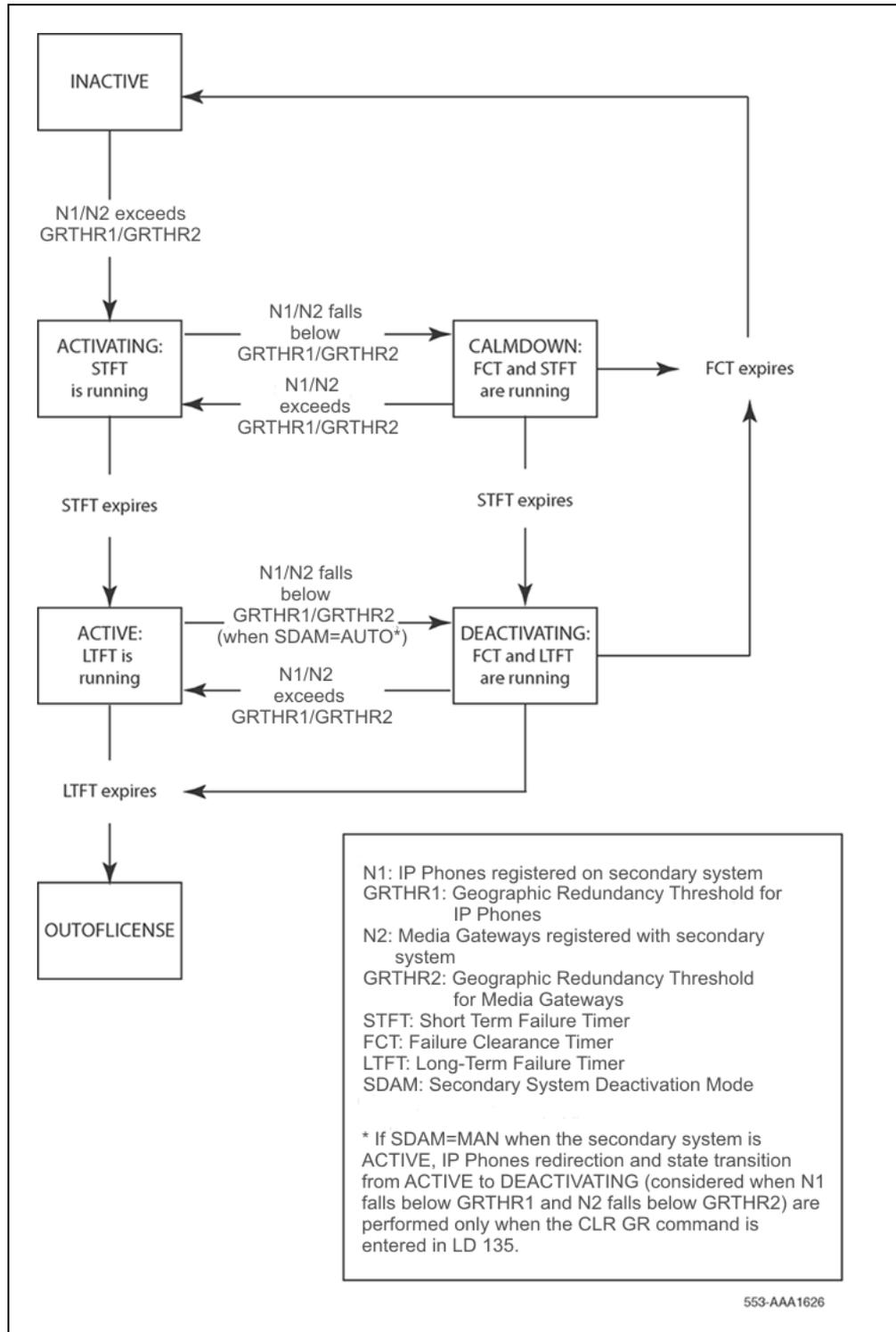


Table 5
Secondary system state control data set

Variable	Definition
N1	Number of IP Phones registered with the secondary system, updated in real time. The secondary system uses this value to monitor primary system health.
N2	Number of Media Gateways registered with the secondary system, updated in real time. The secondary system uses this value to monitor primary system health.
GRTHR1	Geographic Redundancy threshold for IP Phones. This is a customer-definable threshold against which N1 is compared. If the secondary system is INACTIVE and N1 exceeds the GRTHR1, the secondary system escalates to the ACTIVATING state. (GRTHR1 is configurable in LD 117.)
GRTHR2	Geographic Redundancy threshold for Media Gateways. This is a customer-definable threshold against which N2 is compared. If the secondary system is INACTIVE and N2 exceeds the GRTHR2, the secondary system escalates to the ACTIVATING state. (GRTHR2 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 when 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 prevents 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>

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 OUTFLICENSE 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, when 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 N1 falls below GRTHR1 and N2 is below GRTHR2).</p> <p>If SDAM = MAN, the secondary system, when 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 N1 falls below GRTHR1 and N2 falls below GRTHR2, 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 State Control Blocks \(GRSC\) "](#) (page 51).

For details on the recovery of the primary system following a Long-Term Failure, refer to [Procedure 11 "Recovering the primary system database"](#) (page 58).

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 15 minutes. This waiting period eliminates unnecessary state transitions so that IP Phones can re-register to the secondary system. The secondary system can now obtain the appropriate value of IP Phones registered (N1).

OUTFLICENSE state

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

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

If the primary system is active, TDM resources and IP Phones receive services from the primary system (as pointed to by S2).

If the Primary Call Server fails, the TDM resources and IP Phones receive services from Alternate Call Server 1.

If both the Primary and Alternate Call Server 1 Call Servers fail, the TDM resources and IP Phones receive services from Alternate Call Server 2 (local Secondary Call Server pointed to by S1).

If Alternate Call Server 1 is down but the Primary Call Server and Alternate Call Server 2 are active, the TDM resources and IP Phones receive services from the primary system.

If Alternate Call Server 2 is down but the primary system is active, the TDM resources and IP Phones receive services from the primary system.

If the Primary and Alternate Call Server 2 systems are down, the IP Phones cannot connect to Alternate Call Server 2 because S1 and S2 can only be configured for each individual IP Phone.

When its S1 Retry Count expires, the IP Phone uses its S2 value to register directly to the primary system and receive service. TDM resources continue to provide service according to the triple IP registration settings. If connectivity to the Primary server is lost while the Secondary Call Server is in a failed state, the resources attempt to connect to the Secondary Call Server defined as Alternate Call Server 2.

To ensure that Geographic Redundancy is available when required, you must correct the secondary system fault and restore the system.

Network connectivity failure call scenarios

[Table 6 "VNR and NRS routing when Primary Call Server fails" \(page 36\)](#) and [Table 7 "VNR and NRS routing when Primary Call Server is active but unreachable" \(page 36\)](#) show how NRS and VNR handle various calls when connectivity has failed due to Primary Call Server failure and network issues.

When the Primary Call Server fails, VNR and NRS respond as shown in Table 6 "VNR and NRS routing when Primary Call Server fails" (page 36)

Table 6
VNR and NRS routing when Primary Call Server fails

	Call originator	Call destination	Call treatment
Internal calls	IP Phone registered on a Secondary CS in the system TDM telephone configured on an MG registered to a Secondary CS in the system	IP Phone registered on a different Secondary CS in the system TDM telephone configured on an MG registered to a different Secondary CS in the system	VNR routes incoming calls to a Secondary CS (Alternate Call Server 1 or Alternate Call Server 2)
Incoming external calls	Any telephone on a non-Geographic Redundant system	IP Phone registered on a Secondary CS in the system TDM telephone configured on an MG registered to a Secondary CS in the system	NRS routes incoming external calls to a Secondary CS (Alternate Call Server 1 or Alternate Call Server 2)

In the event that connectivity problems allow some Secondary Call Servers to communicate with the primary system while others cannot, VNR and NRS route the calls as shown in Table 7 "VNR and NRS routing when Primary Call Server is active but unreachable" (page 36).

Table 7
VNR and NRS routing when Primary Call Server is active but unreachable

	Call originator	Call destination	Call treatment
Internal calls	IP Phone registered on active Secondary CS in the system TDM telephone configured on an MG registered to active Secondary CS in the system	IP Phone registered on Primary CS TDM telephone configured on an MG registered to Primary CS	VNR routes calls to a Secondary CS (Alternate Call Server 1 or Alternate Call Server 2)
	IP Phone registered on active Secondary CS in the system	IP Phone registered on a different Secondary CS in the system	NRS routes calls to Primary CS, which responds according to HUNT or CFNA settings

	Call originator	Call destination	Call treatment
	TDM telephone configured on an MG registered to active Secondary CS in the system	TDM telephone configured on an MG registered to a different Secondary CS in the system	
	IP Phone registered on Primary CS TDM telephone configured on an MG registered to Primary CS	IP Phone registered on active Secondary CS in the system TDM telephone configured on an MG registered to active Secondary CS in the system	NRS routes calls to Primary CS, which responds according to HUNT or CFNA settings
Incoming external calls	Any telephone configured on a non-Geographic Redundant system	IP Phone registered on Primary CS TDM telephone configured on an MG registered to Primary CS	NRS routes call to Primary CS
	Any telephone configured on a non-Geographic Redundant system	IP Phone registered on active Secondary CS in the system TDM telephone configured on an MG registered to active Secondary CS in the system	NRS routes calls to Primary CS, which responds according to HUNT or CFNA settings

Survivable Media Gateway planning

For a Survivable Media Gateway configuration, plan the Primary and secondary systems as normal. Refer to the list of Call Servers that support this feature as shown in [Table 1 "Survivable Media Gateway supported CPU types"](#) (page 24).

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

Common CS 1000E planning considerations

In a Survivable Media Gateway configuration, the secondary systems do not have to be duplicates of the primary system. The secondary system provides redundancy for traditional TDM line and analog line cards, including TDM equipment for providing digital media services to the IP Phones such as music and RAN.

The following are considerations to make when planning a Survivable Media Gateway configuration.

Signaling Servers

The secondary CS 1000E systems, like the primary system, must have Signaling Servers installed to provide service to IP Phones. Configure Signaling Servers at the secondary site 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, install fewer Signaling Servers at the Secondary site. When this is the case, you can install enough Signaling Servers to handle the traffic created when the secondary system becomes active.

For more information about Signaling Server capacity, see *Communication Server 1000E Planning and Engineering (NN43041-220)* and *Signaling Server Installation and Commissioning (NN43001-312)*.

Voice Gateway channels

The voice gateway channels are also called DSP channels or the cards physical TNs. For more information about configuring Voice Gateway channels, see *Communication Server 1000E Installation and Commissioning (NN43041-310)*.

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, install each NRS in a different location. Install one NRS with each system or install 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 additional information on installing and configuring the Primary and Alternate NRS, see *IP Peer Networking Installation and Commissioning (NN43001-313)*.

NCS

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

You must configure NCS properties 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. For more information, see *IP Peer Networking Installation and Commissioning (NN43001-313)*.

Vacant Number Routing

You must configure Vacant Number Routing (VNR) 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.

Network Time Protocol

The Network Time Protocol (NTP) is used to synchronize computer clocks in the global IP network. NTP provides a comprehensive mechanism to access the national time and frequency dissemination services, organize the time-synchronization subnet, and adjust the local clock in each participating subnet peer.

Because the parameters for NTP depend upon the geographic location, the NTP parameters stored on the Primary Call Server cannot be replicated to the Secondary Call Server as it is in a different geographic location. The NTP parameters are stored in a separate database file that is not replicated to the Secondary Call Server. Therefore, an NTP configuration does not survive a geographic redundancy switchover.

For more information about Network Time Protocol, see *Features and Services Fundamentals (NN43001-106)*

Time of Day clock

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

Network considerations

The Primary and secondary systems must comply with network requirements as described in *Converging the Data Network with VoIP Fundamentals (NN43001-260)*. In addition, install the Primary and

secondary system TLANs in different LAN/WAN subnets; however, you can install both systems in the same ELAN subnets. The systems must use the same NRS for routing.

The maximum round-trip delay on the IP network between Call Servers and Media Gateways is 80 ms, with a maximum allowable packet loss of 0.5% (0% is recommended).

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 that you install Contivity (or similar security solution) between the ELAN FTP ports of the Primary and secondary systems to ensure the security of the database transfer.

Survivable Media Gateway configuration

Before configuring a system for Survivable Media Gateway, a CS 1000E must already be installed as the primary system. For information on installing and configuring a CS 1000E Call Server, see *Communication Server 1000E Installation and Commissioning (NN43041-310)*. For information on upgrading a CS 1000E system, see *Communication Server 1000E Upgrades (NN43041-458)*.

Follow the steps in [Procedure 1 "Configuring a Survivable Media Gateway system" \(page 40\)](#) to configure Geographic Redundancy: Survivable Media Gateway on the Primary Call Server.

Procedure 1

Configuring a Survivable Media Gateway system

Step	Action
------	--------

- | | |
|---|---|
| 1 | Install the Primary Call Server. <ul style="list-style-type: none">• Install hardware (if required).• Install CS 1000 Release 5.0 software, including GRPRIM package.• Configure IPMGs and Signaling Servers.• Configure NRS.• Install the customer database (if required). |
|---|---|

For more detailed instructions on how to setup and configure a CS 1000E system, see *Communication Server 1000E Installation and Commissioning (NN43041-310)* .

- 2 Configure the primary system for Survivable Media Gateway. For more information, see "[Configuring the primary system](#)" (page 42).
- 3 Install secondary system on existing IPMG:
 - Install hardware (if required).
 - Install software, including GRSEC package.
 - 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 fails.
 - Set up the secondary system specific customer database (very limited data is required):
 - Configure Ethernet Protocol in LD 117.
 - Configure Point-to-Point protocol in LD 117, if needed.
 - Configure Event Preference Table (EPT).

For more detailed instructions on how to setup and configure a CS 1000E system, see *Communication Server 1000E Installation and Commissioning (NN43041-310)* .

- 4 Install and configure the Media Gateway Controllers.
- 5 Install and configure the Media Cards.
- 6 Install and configure the Signaling Servers.
- 7 Install the Primary and Alternate NRS and configure IP Peer Networking. For more information, see *IP Peer Networking Installation and Commissioning (NN43001-313)*.
- 8 On the primary system, perform a data dump (EDD) by using the BKR command in LD 43 and specifying the backup rule associated with each Secondary Call Server.
- 9 On each secondary system, perform the following:
 - Log out from the system and wait until message SRPT4643 is displayed. This message notes the arrival of a new backup data file. Otherwise, after the manual restore and sysload, another automatic restore can occur (if ARSTR is defined YES) followed by an automatic sysload (if SYSLOAD is defined YES).

- Define Backup Rule 1 on the secondary for restoring the first database received from the primary system.
 - Define GRDRC Block with: Rule for BKUP =1, Rule for Restore = 1, ARSTR = NO, ASYSLD = NO. For more information, see "Configure Database Replication Control Block (GRDRC) " (page 48).
 - 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 (all system-specific data is filtered).
 - Perform a manual sysload to endorse the backup database.
- 10** Install (if required) and configure the IP Phones with S1 pointing to the secondary node TPS and S2 pointing to the primary system node TPS. For more information, see *Communication Server 1000E Installation and Commissioning (NN43041-310)* for instructions on installing IP Phones.

—End—

Configuring the Primary Call Server

To configure the Primary Call Server, you must complete all of the following tasks:

- "Configure a Backup Rule (BKR)" (page 42)
- "Configure a Backup Schedule (BKPS)" (page 45)
- "Configure SECRET string for database replication" (page 49)
- "Configure Database Replication Control Block (GRDRC) " (page 48)
- "Configure State Control Blocks (GRSC) " (page 51)

Configure a Backup Rule (BKR)

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.

You can have 1 to 512 defined backup rules if the system is defined to use automatic schedule (SCHD); otherwise, the limit is 100 rules.

You can configure the following rule types:

- RMD: Removable Media Device

- FMD: Fixed Media Device
- SCS: Secondary Call Server
- FTP: File Transfer Protocol

Only 1 rule of type RMD and FMD can be defined for each Secondary Call Server IP address. Up to 50 rules of type SCS can be defined.

To complete the database replication successfully, the Backup Rule must be referenced in the Database Replication Control Block. The secondary also uses the Backup Rule during the database-restore operation to identify the appropriate database to restore.

You can configure the backup rules in the CLI using LD 117 or in Element Manager.

LD 117: Configure a Backup Rule

Command	Description
NEW/CHG BKPR xxx aaa b...b yy	<p>Add (or change) a backup rule, where:</p> <ul style="list-style-type: none"> • xxx = backup rule number ID = 1-100 (this limit increases to 512 if SCHED is configured in GRDRC block for ABKUP field). • aaa = rule type. The options for this parameter are: <ul style="list-style-type: none"> — RMD [<N of versions 1-10> [<name>] — FMD [<N of versions 1-10> [<name>] — FTP <IP addr><login><pwd><path> [<N of versions 1-10> [<name>] — SCS <IP addr of SCS> [<N of versions 1-10> [<name>] <p>Only 1 backup rule can be defined for type RMD or FMD. Only 1 rule of type SCS can be defined for each secondary system IP address (for up to 50 Secondary Call Servers).</p> <ul style="list-style-type: none"> • b...b = ELAN network interface IP address of the destination system. • yy = the number of database versions to save on the destination system = 1-(2)-10.

Command	Description
OUT BKPR xxx	Remove backup rule, where:
PRT BKPR xxx	Print backup rule, where:
	<ul style="list-style-type: none"> xxx = backup rule number ID = 1-100 (this limit increases to 512 if SCHED is configured in GRDRC block for ABKUP field).
	<ul style="list-style-type: none"> xxx = backup rule number ID = 1-100 (this limit increases to 512 if SCHED is configured in GRDRC block for ABKUP field).
	If no rule number is entered, all backup rules are printed.

Configure a Backup Rule in Element Manager

Configure backup rules in Element Manager as follows:

Procedure 2

Configuring a Backup Rule in Element Manager

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Element Manager navigator menu, select Tools > Backup and Restore > Call Server > Backup Rules .
The Backup Rules Web page appears. |
| 2 | To add a Backup Rule, click the Add button.
The Add Backup Rule Web page appears. (To edit a Backup Rule, click the number of the rule to be edited under the Rule Number column.) |
| 3 | Configure the Backup Rule as follows: <ul style="list-style-type: none"> In the Rule Name box, enter a name for the rule. In the IP address box, enter the ELAN network interface IP address of the destination system for the database replication. In the Number of versions kept box, choose the number of database versions to save on the destination system. |
| 4 | Click Save . |

—End—

Configure a Backup Schedule (BKPS)

The backup schedule allows the user to create a schedule where they can specify times for the system to initiate system backups. Backup schedules can be created using the CLI in LD 117 or in Element Manager.

LD 117: Configure a Backup Schedule

Command	Description
NEW/CHG BKPS xxx yyy [<FREQ><DAY><HOUR><MINUTE>]	<p>Add (or change) a new backup schedule, where:</p> <ul style="list-style-type: none"> • xxx = backup schedule number ID = 1-10 (upper limit increases to 512 if SCHED is configured in GRDRC block for ABKUP field). • yyy = number of the backup rule for the scheduled backup operation. • FREQ = defines how often the backup takes place. The options for this parameter are: <ul style="list-style-type: none"> — M = monthly — W = weekly — D = daily — Triggered by EDD = Triggered by Equipment Data Dump (this option is not available when Automatic Backup field is configured as ABKP = SCHED). • DAY = This parameter is dependant upon the entry for FREQ. <ul style="list-style-type: none"> — If M was selected for FREQ, this value is (1)-31. — If W was selected for FREQ, this value is one of SU / MO / TU / WE / TH / FR / SA. — If D was selected for FREQ, this value is represented by the next parameter, HOUR. • HOUR = 0-(3)-23. • MINUTE = (0)-59.

Command	Description
OUT BKPS xxx	Remove backup schedule, where:
PRT BKPS xxx	Print backup schedule, where:

Configure a Backup Schedule in Element Manager

To configure a backup schedule in Element Manager, do the following:

Procedure 3

Configuring a Backup Schedule in Element Manager

Step	Action
1	From the Element Manager navigator menu, select Tools > Backup and Restore > Call Server > Backup Schedules . The Backup Schedules Web page appears.
2	To add a new backup schedule, click Add . The Add Web page appears.
3	Configure the backup schedule as follows: <ul style="list-style-type: none"> In the Backup Schedule Number box, enter the schedule number. If Automatic Replication Backup is defined as SCHD during GRDRC configuration, the range is 1 to 512. Otherwise, the default range is 1 to 10. Choose the appropriate value from the Backup Rule drop-down list. Choose the appropriate values from the Frequency, Day, Hour, Minute, and Triggered by EDD lists as required.
4	Click Save .

—End—

You can edit a backup schedule by selecting the number of the rule to be edited under the Schedule Number column.

Configure Database Replication Control (GRDRC) block

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.

The GRDRC block is configured in LD 117 using CLI or in Element Manager.

LD 117: Configure GRDRC block

Command	Description
NEW/CHG GRDRC xxx aaa yyy bbb ccc	<p>Add (or change) 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"> — SCHED—according to defined backup schedule — 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 (ARSTR) is allowed. • ccc = (YES)/NO. Defines whether or not the automatic sysload after successful automatic restore (ASYSLD) is allowed. ccc = YES is only allowed if bbb = YES.
OUT GRDRC	Remove current GRDRC Block.
PRT GRDRC	Print GRDRC Block.

Configure GRDRC block in Element Manager

To configure the GRDRC block in Element Manager, perform the following procedure.

Procedure 4
Configuring GRDRC block in Element Manager

Step Action

- 1 From the Element Manager navigator menu, select **System > Geographic Redundancy > Database Replication Control**.
 The **Database Replication Control** Web page appears.
 (If no backup rule of type SCS is configured, a message appears asking if you want to configure one. Clicking **Ok** opens the **Backup Rules** page. GRDRC options are not available for configuration unless a backup rule of type SCS exists.)
 If no GRDRC block has been configured, a message appears confirming that you want to create one.
- 2 Click **Ok**.
- 3 Select the **GRDRC** check box.
 The GRDRC configuration options are available (not dimmed).
- 4 Select the desired **Rule Number for Backup and Restore**
- 5 Choose the **Automatic Replication Backup** value from the list.
- 6 To enable the automatic restore operation, select the **Automatic Replication Restore** check box.
- 7 To allow the automatic sysload operation, select the **Automatic Sysload** check box.
- 8 Click **Save**.
- 9 To delete a GRDRC block, clear the GRDRC check box and click **Save**.
 The GRDRC block is deleted.

—End—

Configure SECRET string for database replication

The SECRET string is a pre-shared security password enabling the Secondary Call Servers to decrypt the database sent from the Primary Call Server. Each Call Server in the system must have the same SECRET string password for database replication to be successful.

The SECRET string is configured using LD 117.

Table 8
LD 117: Configure SECRET string for database replication

Command	Description
SECRET SET GR <GR SECRET string>	Define the SECRET string. The following limitations apply: <ul style="list-style-type: none"> • Maximum of 30 characters. • Cannot use the "!" character.
SECRET DEFAULT GR	Restore the SECRET string to the default value.
SECRET OUT GR	Remove the SECRET string.
SECRET STAT GR	Print the SECRET string.

Configure SECRET string in Element Manager

The SECRET string is a pre-shared security password enabling the Secondary Call Servers to decrypt the database sent from the Primary Call Server. Each Call Server in the system must have the same SECRET string password for database replication to be successful.

To configure the SECRET string in Element Manager, perform the following procedure.

Procedure 5

Configuring SECRET string in Element Manager

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Element Manager navigator menu, select System > Geographic Redundancy > Database Replication Control . |
|---|--|

The **Database Replication Control** Web page appears.

- | | |
|---|--|
| 2 | Configure the SECRET string in one of the following ways: <ol style="list-style-type: none"> To configure the SECRET string with the default password, select the Revert to default check box. Click Save.
The SECRET string is saved with the default value. |
|---|--|

Or

- | | |
|----|---|
| b. | To configure a new SECRET string value, clear the Revert to default check box. Enter a new value in the Secret Password box. The new password must conform to the following limitations: <ul style="list-style-type: none"> • Maximum of 30 characters. • The "!" character cannot be used. |
|----|---|

Click **Save**.

The SECRET string is configured with the new value.

- 3 To remove the SECRET string value, clear the **Secret String** check box and click **Save**.

The SECRET string value is removed.

—End—

Configure State Control (GRSC) Blocks

The Geographic Redundancy State Control (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](#)" (page 31).

Each Secondary Call Server must have its own GRSC block configured. The system supports up to 512 configured GRSC blocks.

LD 117: Configure GRSC blocks

Command	Description
NEW/CHG GRSC <associated scs>[<GRTHR1><GRTHR2><STFTO><FCTO><SDAM>]	<p>Add (or change) a new GRSC block, where:</p> <ul style="list-style-type: none"> • associated scs—Secondary Call Server to be associated with the GRSC block, where: <ul style="list-style-type: none"> — Backup Rule Number—number of the SCS backup rule configured. — NBKP—defines a generic GRSC block for Secondary Call Servers that do not have an associated backup rule configured. — ALL—automatically configures GRSC blocks for all Secondary Call Servers that have associated backup rule defined. • GRTHR1—the number (N) of IP Phones that must register on the secondary system for the system to escalate to the ACTIVATING state. <p>If no value is entered, xxx = 1. The maximum value of xxx is: 10% x (Basic IP User license + IP User license).</p> • GRTHR2—the defined threshold for the number of Media Gateways registered to the Secondary Call Server. If the secondary system is INACTIVE and the number of Media Gateways registered exceeds GRTHR2, the system escalates to the ACTIVATING state.

Command	Description
OUT GRSC <associated scs>	<ul style="list-style-type: none"> STFTO—Short Term Failure Timer, in minutes = (5) - 600. FCTO—Failure Clearance Timer, in minutes = (5) - 180. SDAM—Secondary system Deactivation Mode = (AUTO)/MAN. <p>Remove GRSC Block, where:</p> <ul style="list-style-type: none"> <associated scs>—Secondary Call Server to be associated with the GRSC block, where: <ul style="list-style-type: none"> Backup Rule Number—number of the SCS backup rule configured. NBKP—defines a generic GRSC block for Secondary Call Servers that do not have an associated backup rule configured. ALL—automatically configures GRSC blocks for all Secondary Call Servers that have associated backup rule defined.
PRT GRSC [(ALL)/<associated scs backup rule>/NBKP]	<p>Print GRSC Block, where:</p> <ul style="list-style-type: none"> ALL—all Secondary Call Servers that have backup rules defined. associated scs backup rule—number of the SCS backup rule configured. NBKP—a generic GRSC block for Secondary Call Servers that do not have an associated backup rule configured.

Configure GRSC block in Element Manager

To configure the GRSC block in Element Manager, do the following:

Procedure 6

Configuring GRSC block in Element Manager

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Element Manager navigator menu, select System > Geographic Redundancy > State Control .
The State Control Web page appears. |
| 2 | To add a new GRSC block, click the Add button. To edit a GRSC block, click the link under the Associated SCS column.
The Add State Control Web page appears. |
| 3 | Choose the appropriate item from the Associated Secondary Call Servers list. |
| 4 | Enter the desired IP Phone threshold number in the Threshold1 box. |

- 5 Enter the desired Media Gateway threshold number in the **Threshold2** box.
- 6 Enter the number of minutes in the **Short Term Failure Timeout** box.
- 7 Enter the number of minutes in the **Fault Clearance Timeout** box.
- 8 Choose the deactivation mode from the **Secondary CS Deactivation Mode** list.
- 9 Click **Save**.

—End—

Configure the Media Gateway Controller (MGC)

Package 404 or 405 must be enabled to configure the Media Gateway Controller in Element Manager.

Note: Configure the Media Gateway Controllers on the Primary Call Server. The settings are included with database replication to the Secondary Call Servers.

To configure the Media Gateway Controller in Element Manager, do the following:

Procedure 7

Configuring the Media Gateway Controller in Element Manager

Step	Action
1	From the Element Manager navigator menu, select System > IP Network > Media Gateways . The Media Gateways Web page appears.
2	From the list of IPMGs, click the MGC link (under the Type column) for the device to be configured. The IPMG 4 0 Media Gateway Controller (MGC) Configuration Web page appears.
3	Click [+] to expand the LAN configuration section. If Package 404 is enabled, the Primary Call Server IP is identical to the Call Server that Element Manager is managing and appears dimmed (read-only).
4	Enter IP values for the Primary Call Server, Alternate Call Server 1, and Alternate Call Server 2 in the appropriate boxes.

- 5 Fill in any other mandatory boxes (mandatory boxes are marked with an asterisk [*]).
- 6 Click **Submit**.

—End—

For more information about the installation and configuration of the Media Gateway Controller, see *Communication Server 1000E Installation and Commissioning (NN43041-310)*.

For a complete list of available Media Gateway Controller commands, see *Software Input/Output Administration (NN43001-611)*.

Configure IP telephony nodes

Package 404 or 405 must be enabled to configure IP telephony nodes in Element Manager. To configure IP telephony nodes in Element Manager, do the following:

Procedure 8

Configuring IP telephony nodes in Element Manager

Step	Action
1	From the Element Manager navigator menu, select System > IP Network > Nodes: Servers, Media Cards . The Node Configuration Web page appears.
2	Select Edit for an existing node. The Edit Web page appears.
3	From the element list, click the Add beside the Cards element. The Cards element expands to display the Card properties.
4	Select the Card processor type from the list. If Pentium Card is selected, the IP fields for Primary Call Server, Alternate Call Server 1, and Alternate Call Server 2 are not displayed. If Voice Media Gateway or MC 32S card are selected, the IP fields for Primary Call Server, Alternate Call Server 1, and Alternate Call Server 2 are displayed. If Package 404 is enabled, the Primary Call Server IP is identical to the Call Server that Element Manager is managing and appears dimmed (read-only).

- 5 Enter the IP values for the Primary Call Server, Alternate Call Server 1, and Alternate Call Server 2 in the appropriate boxes.
- 6 Fill in any other mandatory boxes (mandatory boxes are marked with an asterisk [*]).
- 7 Click **Save and Transfer**.

—End—

Configure Primary (S1) and Secondary (S2) Connect Servers

To install and configure IP Phones, refer to *Communication Server 1000E Installation and Commissioning (NN43041-310)*. Ensure the S1 of each IP Phone points to the local secondary system node TPS, and the S2 points to the primary system node TPS.

To configure IP Phones using DHCP, refer to *Converging the Data Network with VoIP Fundamentals (NN43001-260)*.

Adding a new Secondary Call Server to the system

You can configure up to 50 additional Secondary Call Servers for a Survivable Media Gateway configuration. To add a Secondary Call Server to the system, do the following:

Procedure 9

Adding a new Secondary Call Server to the system

Step	Action
------	--------

- | | |
|---|--|
| 1 | <p>On the new Secondary Call Server:</p> <ul style="list-style-type: none"> • Install the hardware (if required). • Install CS 1000 Release 5.0 (same version as Primary or later). • Configure the Call Server with system specific data, such as IP address, Signaling Server settings, and so forth. |
|---|--|

For more information about installing and configuring a CS 1000E system, see *Communication Server 1000E Installation and Commissioning (NN43041-310)*

- | | |
|---|--|
| 2 | <p>On the Primary Call Server, configure the following for each new Secondary Call Server:</p> <ul style="list-style-type: none"> • Backup Rule (see "Configure a Backup Rule (BKR)" (page 42)). • Backup Schedule (see "Configure a Backup Schedule (BKPS)" (page 45)). |
|---|--|

- State Control Block (see ["Configure State Control Blocks \(GRSC\) "](#) (page 51)).

For each Secondary Call Server, use the BKR command in LD 43 (specifying the associated backup rule) to replicate the database. For more information, see ["Manual database replication and restore"](#) (page 60).

- 3 On the new Secondary Call Server:
 - After replicating the backup set from the Primary Call Server, define Backup Rule 1. For more information, see ["Configure a Backup Rule \(BKR\)"](#) (page 42).
 - In LD 43, use the RSR 1 command to manually restore the database from the Primary Call Server backup set. (Filtering of primary system specific data must be used.)
 - Sysload the Call Server.

—End—

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 \(GRDRC\) "](#) (page 48)). This prevents the automatic restore process from accidentally overwriting the latest changes made on the secondary system.

The secondary system administrative changes can 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 and N1 falls below GRTHR1 and N2 falls below GRTHR2, the system transitions to the DEACTIVATING state. It also sends a switch to Primary request to all Media Gateway Controllers registered on the Secondary Call Server.

Clear ACTIVE state in Element Manager

To clear the secondary system ACTIVE state in Element Manager, do the following.

Procedure 10**Clearing secondary system ACTIVE state in Element Manager**

Step	Action
1	In the Element Manager navigator tree, select System > Maintenance > Select by Overlay > LD 135—Core Common Equipment Diagnostics > Geographic Redundancy Diagnostics . The Geographic Redundancy Diagnostics Web page appears.
2	Click the Clear GR button. The ACTIVE state for the Secondary Call Server is cleared.

—End—

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 after it returns to normal operations.

[Procedure 11 "Recovering the primary system database" \(page 58\)](#) describes how to perform a system recovery following primary system failure.

Procedure 11
Recovering the primary system database

Step Action

- 1 On the secondary system:
 - a. Define a new Backup Rule in LD 117 using the IP address of the primary system. For more information, see ["Configure a Backup Rule \(BKR\)"](#) (page 42).
 - 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. 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. For more information, see ["Manual database replication and restore"](#) (page 60).

- 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. System-specific data for the primary system is filtered.

This manually restores the database that was just transferred to the primary system.
 - b. Perform a sysload to accept the newly restored data.

—End—

Procedure 12 ["Testing the recovered primary system"](#) (page 59) describes how to perform a system test following primary system recovery.

Procedure 12
Testing the recovered primary system

Step	Action
1	<p>On the primary system:</p> <p>a. In LD 117, enter the following:</p> <pre>CHG GRDRC <BKUP rule> IMM <Rule for Restore> YES YES</pre> <p>where</p> <p><BKUP rule> and <Rule for Restore> are both the original Backup Rule for replication to the secondary system (not the rule defined in Procedure 11 "Recovering the primary system database" (page 58).</p> <p>b. Perform a data dump in LD 43.</p> <p>The data dump initiates the automatic database replication to the secondary system.</p>
2	<p>On the secondary system:</p> <p>a. In LD 117, define ARSTR = YES and ASYSLD = YES in the GRDRC data.</p> <p>b. Log out of the system and wait for the automatic restore and automatic sysload to take place, then accept the backup database.</p>

—End—

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.

Upgrade the secondary system first, and then the primary system. This allows the database replication process to function normally during the upgrades. The secondary system performs 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 5.0 software.

Maintenance

The Primary and secondary systems conform to the methods and procedures used for local and remote access as defined for CS 1000E systems. All systems conform to the existing methodologies used to deploy maintenance and diagnostic patches for CS 1000 Release 5.0 software.

Geographic Redundancy: Survivable Media Gateway preserves all existing VxWorks or overlay support tools available in CS 1000 Release 5.0 software for CS 1000E systems, except where otherwise noted in this document.

TM 3.1

TM 3.1 can be used to administer the Primary and secondary systems in a Survivable Media Gateway configuration. The Primary and secondary systems are represented in TM 3.1 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 TM 3.1 by cloning the primary system data and 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 TM 3.1.

Manual database replication and restore

The database replication and restore procedures are initiated using LD 43.

LD 43: Manual database replication

Command	Description
BKR xx	Invoke database-replication operation, where: <ul style="list-style-type: none">xx = Backup Rule number.

Command	Description
RSR xx yy	<p>This command is typically entered on the primary system for replication to the secondary system.</p> <p>Restore the database, where:</p> <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 GRDRC block; otherwise, all system-specific definitions are lost. • yy = database version number. If no version number is entered, the most recent backup (1) is used. <p>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.</p> <p>This command is typically entered on the secondary system to restore a database received from the primary system.</p> <p>When the RSR command is issued, the following confirmation prompt appears:</p> <ul style="list-style-type: none"> • Perform IP Config filtering (Y / N)? <p>If the user enters Y, the database is restored without the system-specific data.</p> <p>If the user enters N, the database is restored with the system-specific data and any existing system-specific data is overwritten.</p>

Manual database restore in Element Manager

To initiate the database replication manually using Element Manager, do the following.

Procedure 13

Manual database restore in Element Manager

Step	Action
1	From the Element Manager navigation tree, select Tools > Backup and Restore > Call Server > Restore .
2	Select Restore According to Rule from the list. The configured backup rules and restore versions are displayed.
3	Select the Apply Filtering check box to filter system-specific data. This restores the file without the system-specific data that is automatically included with the compressed file sent from the Primary Call Server. If not selected, the system-specific data

from the restore file is included with the restored information and overwrites any existing system-specific data on the Secondary Call Server.

System-specific data includes IP addresses, netmasks, routes, nodes, and EPT information included with the compressed backup file sent from the Primary Call Server.

- 4 Click **Submit**.

—End—

Diagnostics

System status

The status of each system in the Survivable Media Gateway 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 the system status for Primary or secondary systems in LD 135 as follows:

LD 135: Survivable Media Gateway system status

Command	Description
STAT GR	The current status of Geographic Redundancy: Survivable Media Gateway on the specified system appears.
STAT IPL xx	Status of the IP link for a specified MG 1000E appears and indicates if it is registered to an Alternate Call Server, where: <ul style="list-style-type: none"> • xx = cabinet number of the Media Gateway queried. <p>Note: You can also use the STAT IPMG command in LD 117 to see more details about IP connection status.</p>
SMGR xx yy	Forces Media Gateway to register on a specified Call Server, where: <ul style="list-style-type: none"> • xx = specified Call Server. Options for this parameter are PRIM (Primary), ALT1 (Alternate Call Server 1), or ALT2 (Alternate Call Server 2). • yy = cabinet number of the Media Gateway to be switched.

Checking system status in Element Manager

To check the system status in Element Manager, do the following:

Procedure 14

Checking system status in Element Manager

Step	Action
1	From the Element Manager navigation tree, select System > Maintenance > Select by Overlay > LD 135—Core Common Equipment Diagnostics > Geographic Redundancy Diagnostics . The Geographic Redundancy Diagnostics Web page appears.
2	Click Status . The system status for Survivable Media Gateway configuration displays. You can also check the status of individual system components.
3	Choose an item from the More Actions list.
4	Click Execute . The status of the selected item is displayed in the results area. If the results area displays a list (for example, of IP addresses for configured Media Gateways or available TNs), selecting the item and clicking Execute displays the status of the individual item.
5	To switch the registration of an item to a different Call Server, choose Register to Primary , Register to Alternate CS1 , or Register to Alternate CS2 from the More Actions list. A confirmation message appears.
6	To confirm the action, click Ok . The item is registered to the new Call Server.

—End—

Testing Survival Media Gateway system in Element Manager

To perform Survival Media Gateway system testing in Element Manager, do the following.

Procedure 15**Testing Survival Media Gateway system in Element Manager****Step Action**

- | Step | Action |
|------|---|
| 1 | From the Element Manager navigation tree, choose System > Maintenance > Select by Overlay >> LD 135 - Core Common Equipment Diagnostics > Geographic Redundancy Diagnostics .
The Geographic Redundancy Diagnostics Web page appears. |
| 2 | From the More Actions list, choose Test GR All . (This option is only available from the Primary Call Server.) |
| 3 | Click Execute . |

—End—

System faults**FTP transfer failure**

During an automatic backup attempt, if the primary system fails to gain FTP access to the pecondary 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).

If a backup attempt fails, the following message 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, to <SCS IP address>
```

When the FTP transfer to the secondary system succeeds, 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 actions are automatically 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
```

Feature interactions

Security

The database replicated from the Primary to Secondary Call Servers is encrypted on the primary system and decrypted on secondary systems using a shared SECRET string. A checksum process is used to compare the files for verification. For more information on database replication security, see "[Configure SECRET string for database replication](#)" (page 49).

For more information on Communication Server 1000 security features, see *Security Management Fundamentals (NN43001-604)*.

Media Security

Survival Media Gateway has an interaction with trunk zone dependant allocation.

System monitoring

SNMP system alarms monitoring

Nortel recommends that you use Simple Network Management Protocol (SNMP) be used for system alarms monitoring. For more information about SNMP, see *Communication Server 1000 Fault Management—SNMP (NN43001-719)*

Geographic Redundancy 1+1 configuration

Contents

This section contains information on the following topics:

"Description" (page 67)

"Upgrading an existing 1+1 configuration to Survivable Media Gateway" (page 67)

Description

1+1 configuration is replaced with Survivable Media Gateway as of CS 1000 Release 5.0. For information relating to 1+1 configurations, refer to previous issues of this document.

Note 1: Existing Geographic Redundancy 1+1 configurations are supported in CS 1000 Release 5.0; however, no new packages or options are available.

Note 2: 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 are not operational if the system fails.

Upgrading an existing 1+1 configuration to Survivable Media Gateway

This section tells you how to upgrade an existing Geographic Redundancy 1+1 configuration to a Survivable Media Gateway configuration. This feature requires CS 1000 Release 5.0 to be installed on the Primary and all Secondary Call Servers. Survivable Media Gateway is not supported for previous versions of the software and is only supported on CS 1000E (CP PIV and CP PM) Call Servers.

For information on system upgrades, see the following documents as applicable:

- *Communication Server 1000E Upgrade—Option 11C Cabinet to CS 1000E (NN43041-464)*
- *Communication Server 1000E Upgrade—Option 11C Chassis to CS 1000E (NN43041-465)*
- *Communication Server 1000E Upgrade—CS 1000M Cabinet to CS 1000E (NN43041-466)*
- *Communication Server 1000E Upgrade—CS 1000M Chassis to CS 1000E (NN43041-467)*

To upgrade an existing 1+1 configuration to Survivable Media Gateway, you must complete the following tasks:

- Upgrade the Primary Call Server and all Secondary Call Server to Communication Server 1000 Release 5.0 or higher. For more information on upgrading system software, see *Communication Server 1000E Upgrades (NN43041-458)*.
- On the Primary Call Server, update the Geographic Redundancy configuration for the existing Secondary Call Server.
- On the Primary Call Server, update the Geographic Redundancy configuration for the new Secondary Call Server.
- Replicate the database from the Primary Call Server to each Secondary Call Server.
- On each Secondary Call Server, verify and accept the transferred database.

These tasks are described in more detail in [Procedure 16 "Upgrading an existing 1+1 configuration to Survivable Media Gateway" \(page 68\)](#).

Procedure 16

Upgrading an existing 1+1 configuration to Survivable Media Gateway

Step	Action
1	<p>Upgrade the Primary Call Server to Communication Server 1000 Release 5.0 or higher. The system might indicate that one or all of the following warning conditions exist:</p> <ul style="list-style-type: none"> • Several Secondary Call Server backup rules are configured for a server with the same IP address. • Several RMD backup rules are configured. • Several FMD backup rules are configured.

- 2 On the new Secondary Call Server:
 - Install the hardware.
 - Install Communication Server 1000 Release 5.0 or higher software.
 - Configure the Call Server. For information on configuring a Call Server, see *Communication Server 1000E Installation and Commissioning (NN43041-310)*.

- 3 On the Primary Call Server:
 - Configure the new peripheral equipment.
 - In LD 117, update the Geographic Redundancy configuration for the existing Secondary Call Server by doing the following:
 - Select the RMD, FMD, and SCS backup rule to use and remove the redundant ones.
 - Configure the BKPS block associated with the SCS backup rule. For more information, see "[Configure a Backup Schedule \(BKPS\)](#)" (page 45).
 - Modify the GRDRC block and set the ABKUP field to SCHD. For more information, see "[Configure Database Replication Control Block \(GRDRC\)](#)" (page 48).
 - Modify the GRSC block to associate it with the existing Secondary Call Server and set the proper parameters. For more information, see "[Configure State Control Blocks \(GRSC\)](#)" (page 51).
 - In LD 117, configure the Geographic Redundancy for the new Secondary Call Server by doing the following:
 - Configure the backup rule associated with the new Secondary Call Server. For more information, see "[Configure a Backup Rule \(BKR\)](#)" (page 42).
 - Configure the BKPS block associated with the new Secondary Call Server. For more information, see "[Configure a Backup Schedule \(BKPS\)](#)" (page 45).
 - Configure the GRSC block associated with the new Secondary Call Server. For more information, see "[Configure State Control Blocks \(GRSC\)](#)" (page 51).
 - In LD 43, use the BKR command with the appropriate backup rule to replicate the database to both the old and new Secondary Call Servers. For more information, see "[Manual database replication and restore](#)" (page 60).

- 4 On the new Secondary Call Server:
- Verify that the backup set from the Primary Call Server is received.
 - Define Backup Rule 1. For more information, see "[Configure a Backup Rule \(BKR\)](#)" (page 42).
 - Use the RSR 1 command in LD 43 to manually restore the backup data. It is mandatory to use filtering.
 - Sysload the Call Server to accept the database replication.

—End—

Geographic Redundancy Controlled Load-sharing configuration

Contents

This section contains information on the following topics:

"Description" (page 71)

"Normal operation" (page 72)

"Site 1 system failure" (page 75)

"Site 2 system failure" (page 76)

"Planning a Controlled Load-sharing configuration" (page 77)

"Numbering plan" (page 81)

"Branch Office support" (page 83)

"Installing a Controlled Load-sharing configuration" (page 86)

"Maintenance" (page 88)

"Feature interactions" (page 88)

"System monitoring" (page 88)

Description

The Controlled Load-sharing configuration increases the reliability of CS 1000M 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. If either system fails, the remaining active system can assume control of the IP Phones on the failed system 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 Systems and CS 1000E systems can be backed up by either a CS 1000M System or CS 1000E system.

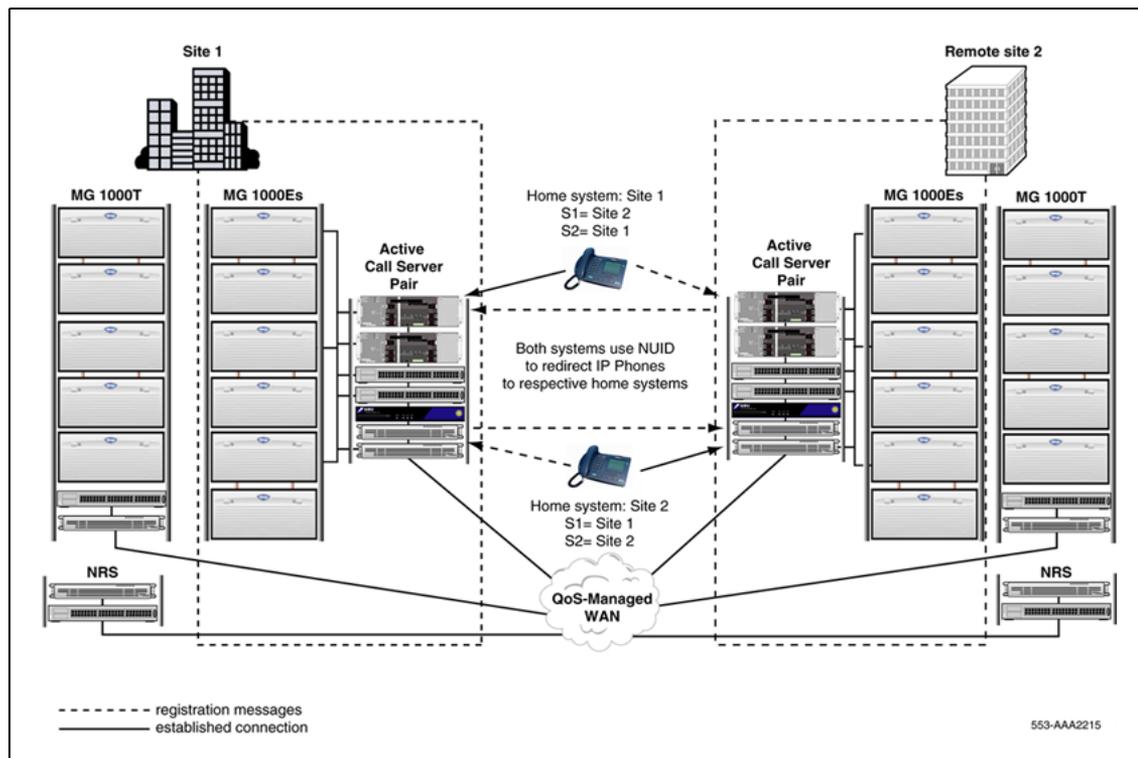
Note 1: The Controlled Load-sharing configuration provides redundancy for IP Phones only. Redundancy for analog (500/2500-type) telephones and digital telephones is not supported. Analog (500/2500-type) and digital telephones can still be connected to a system, but they are not operational if that system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

Note 2: N+1 configuration is not supported with CS 1000 Release 5.0 and later. Systems running N+1 with CS 1000 Release 5.0 and later versions automatically convert to a Controlled Load-Sharing configuration with Temporary IP User license.

Normal operation

Figure 2 "Controlled Load-Sharing configuration" (page 72) shows two CS 1000E systems in a Controlled Load-Sharing configuration.

Figure 2
Controlled Load-Sharing configuration



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

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 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), and 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 2 "Controlled Load-Sharing configuration" \(page 72\)](#), both systems serve 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 Survivable Media Gateway 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.

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 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 Survival Media Gateway and 1+1 configurations, 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.

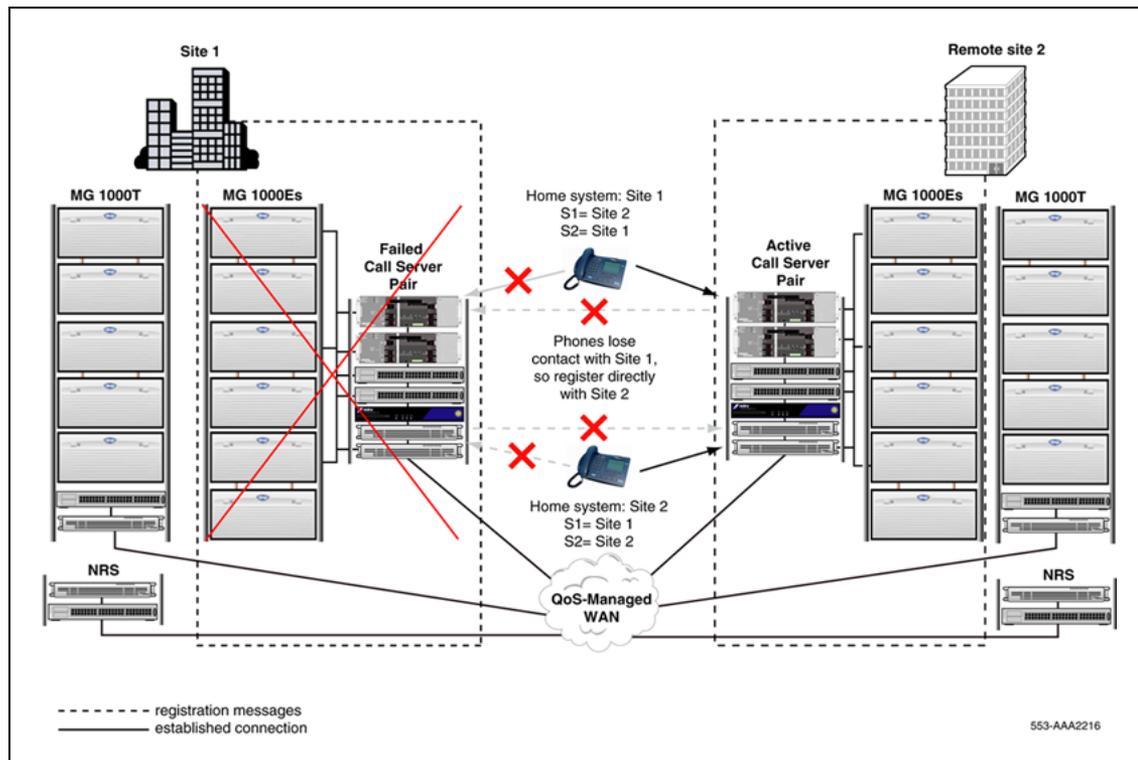
The backup system can be configured to provide the same basic features and services as the home system. This is not a requirement if fewer services on the backup system is acceptable.

Carefully plan the backup system to provide the necessary redundant capacity required. For further planning details, see "Planning a Controlled Load-sharing configuration" (page 77).

Site 1 system failure

Figure 3 "Load-sharing configuration: system failure at Site 1" (page 75) shows a Controlled Load-sharing configuration that is experiencing a failure at Site 1.

Figure 3
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 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 obtain normal service. While they remain registered at Site 2, the IP Phones display "Local Mode".

When 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. When the S1 Retry Count of the IP Phone has expired, the IP Phone 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.

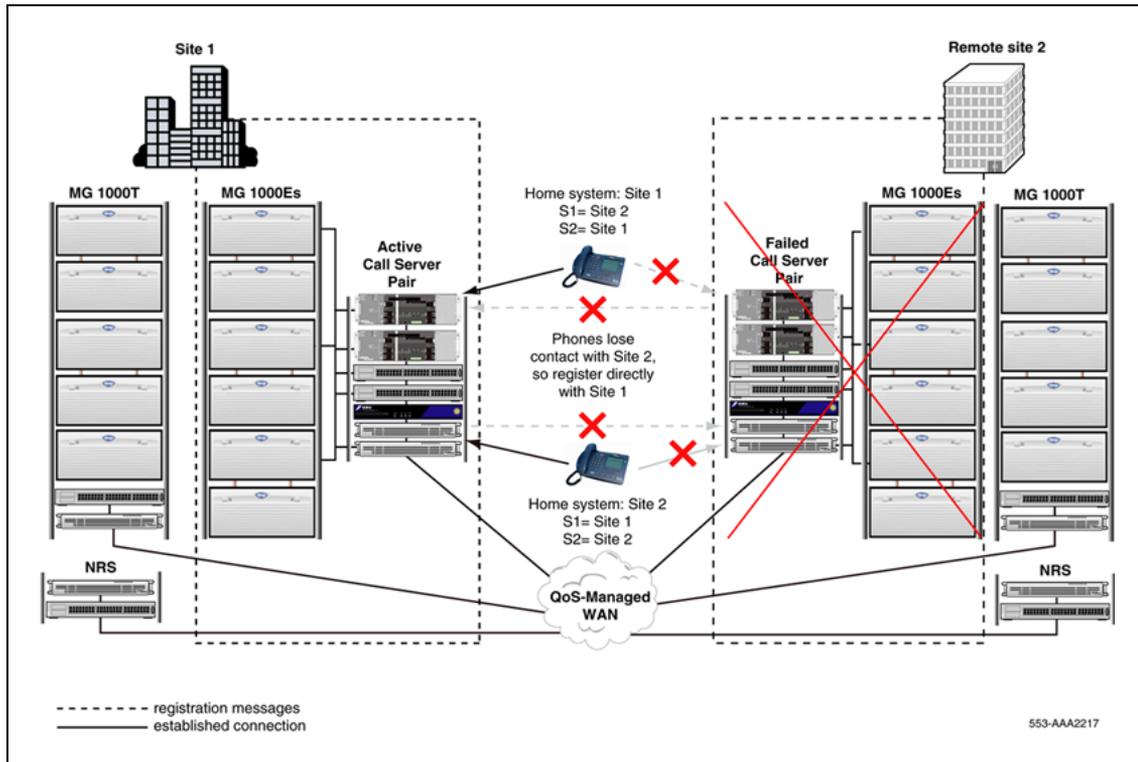
When the IP Phones are registered on Site 2, users have full access to the features and services configured on that system.

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 3 "Load-sharing configuration: system failure at Site 1" (page 75) shows a Controlled Load-sharing configuration that is experiencing a failure at Site 2.

Figure 4
Controlled Load-sharing configuration: system failure at Site 2



Planning a Controlled Load-sharing configuration

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 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 Systems must have Signaling Servers installed 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 (NN43041-220)* and *Signaling Server Installation and Commissioning (NN43001-312)*.

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 (NN43100-500)*.

For example, if the home system node number is 1110, the backup system must use the same leading three digits, 111, in its node number (for example, 1115). The IP Phones must be configured with the same three digits, 111, when defining its Node information. The IP Phone can 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 NRS 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](#)" (page 81). For additional information on installing and configuring the Primary and Alternate NRS refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*.

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

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.

Network Time Protocol

The Network Time Protocol (NTP) is used to synchronize computer clocks in the global IP network. It provides a comprehensive mechanism to access the national time and frequency dissemination services, organize the time-synchronization subnet and adjust the local clock in each participating subnet peer.

Because the parameters for NTP are dependant upon the geographic location, the NTP parameters stored on the Primary Call Server cannot be replicated to the Secondary Call Servers located in a different geographic location. The NTP parameters are stored in a separate database file (ntp.db) which does not get replicated to the Secondary Call Servers. Therefore, an NTP configuration does not survive a geographic redundancy switchover.

For more information about Network Time Protocol, see *Features and Services Fundamentals (NN43001-106)*

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 display the correct time for their area.

For more information, see [Appendix "Controlled Load-sharing zones" \(page 127\)](#).

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.

The following user licenses are available:

Temporary IP User license This IP licensing enhancement limits the number of IP set Terminal Numbers (TN) with Network User ID (NUID) configured. These TNs are not included in the total number of license limitations for IP User, Basic IP User, or ACD agent usage, which makes this option more cost-effective than Basic IP User license or IP User license.

Basic IP User license This license counts IP Phones type 2001 (LD 11, TYPE 2001P2).

IP Users license This license counts IP Phones type 2002, i2210/2211, 2004 and IP Softphone 2050 (LD 11, TYPE i2002, i2210, i2211, i2004, or i2050). If insufficient Basic IP User licenses are available for the IP Phone 2001, the IP User license can also be used for configuration of the IP Phone 2001. When IP User licenses are used to configure the IP Phone 2001, an error message is generated, recommending the purchase of additional Basic IP User licenses.

More information on user licenses for IP Phones is found in *IP Line: Description, Installation, and Operation (NN43100-500)*

Data network planning

The home and backup systems must comply with network requirements as described in *Converging the Data Network with VoIP Fundamentals (NN43001-260)*. The home and backup systems use a common NRS for routing.

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 Reference (NN43001-283)*.

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 DN 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 are 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, $\text{NUID} = \text{AC} + \text{HLOC} + \text{DN}$), 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 DN ranges 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:

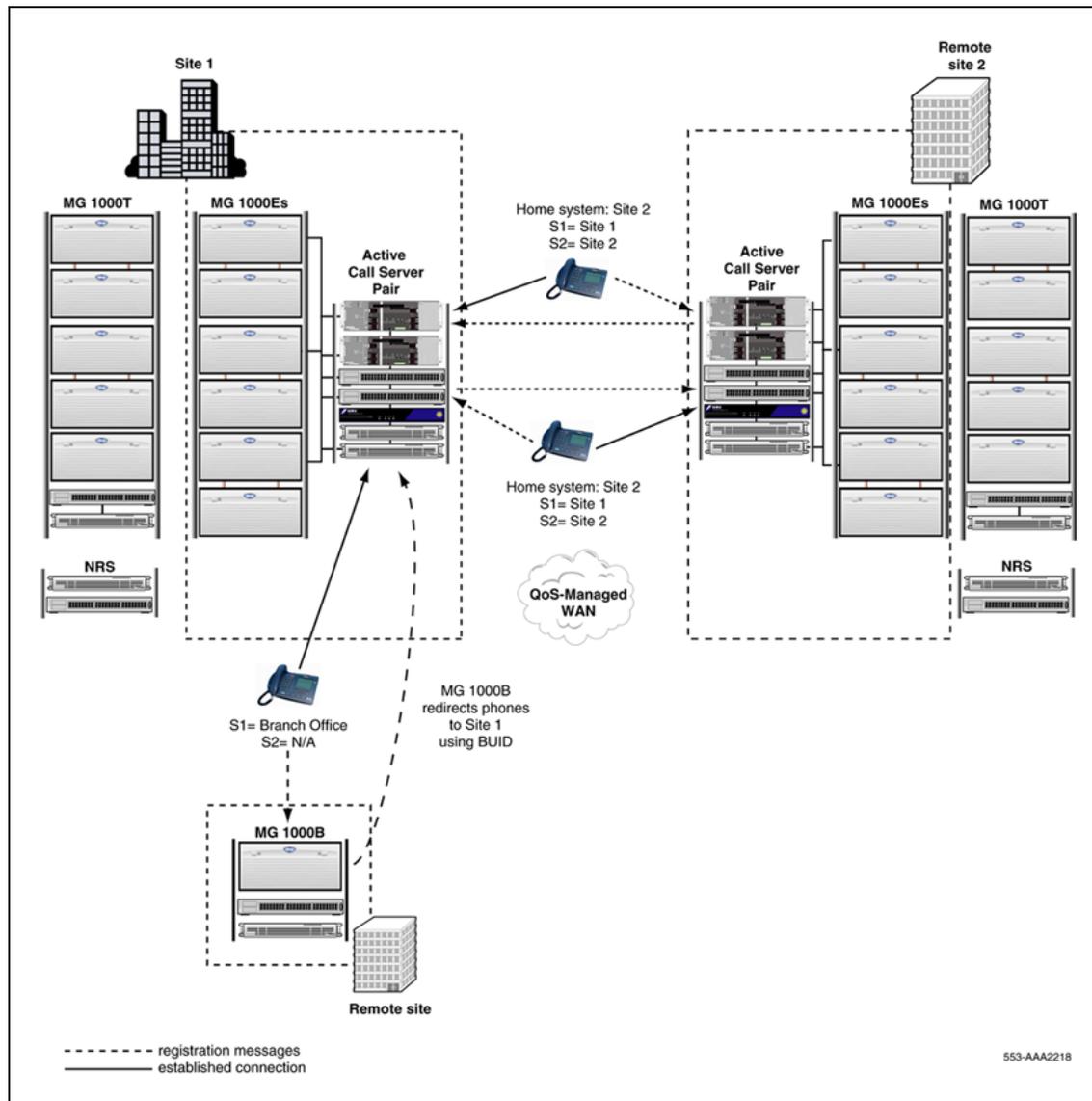
- for home system home-corresponding CDP entry is defined with cost factor 1
- for backup system - cost factor 2
- for branch office - cost factor 3

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 *Branch Office Installation and Commissioning (NN43001-314)*. For the MG 1000Bs to be redundant, each site must use the same TN and DN ranges for the MG 1000B IP Phones.

Figure 5 "Controlled Load-sharing configuration: Branch Office support" (page 84) shows an MG 1000B installed in the Controlled Load-sharing configuration.

Figure 5
Controlled Load-sharing configuration: Branch Office support



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](#)" (page 82). 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: Because 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](#)" (page 82). 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.

Temporary IP User license

This IP licensing enhancement limits the number of IP set Terminal Numbers (TN) with Network User ID (NUID) configured. These TNs are not included in the total number of license limitations for IP User, Basic IP User, or ACD agent usage, which makes this option more cost-effective than IP User license or Basic IP User license.

If the NUID is removed from an existing TN, the Temporary IP Users total is decremented by 1, and the totals for TNs used, IP or Basic IP Users, and ACD agents (if applicable) increment by 1.

Conversely, if the NUID is added to an existing IP set TN, the total of Temporary IP User usage increments by 1, and the totals for TN usage, IP User or Basic IP user usage, and ACD Agent usage (if applicable) are decremented by 1.

IP sets registered with TNs configured with NUID and NHTN are redirected to the Network Home. If the Network home is unreachable, the IP sets stay in Local Mode in their Secondary Call Server. In this situation the IP sets are subject to network wide redundancy Local Mode Licensing restrictions and treatments.

Installing a Controlled Load-sharing configuration

[Procedure 17 "Installing Controlled Load-sharing configuration" \(page 86\)](#) describes the high-level steps required to install a Controlled Load-sharing configuration.

Procedure 17

Installing Controlled Load-sharing configuration

Step	Action
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 <i>IP Peer Networking Installation and Commissioning (NN43001-313)</i> 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—

Provisioning the IP Phones

To install and configure IP Phones, see *Communication Server 1000E Installation and Commissioning (NN43041-310)*. 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 *Converging the Data Network with VoIP Fundamentals (NN43001-260)*.

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	2001P2/2002P1/2002P2	IP Phone type.
	2004P1/2004P2/2050PC	
CUST		Customer number.
	0-99	Range for CS 1000M 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 System and CS 1000E where l = loop, s = shelf, c = card, u = unit.

TM 3.1

The NUID and NHTN values can also be configured using TM 3.1.

Maintenance

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

The Controlled Load-Sharing implementation preserves all existing VxWorks or Overlay support tools available on the CS 1000M System or CS 1000E solutions, except where otherwise noted in this document.

TM 3.1

TM 3.1 can be used to administer the home and backup systems in a Controlled Load-sharing configuration. The home and backup systems are represented in TM 3.1 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 TM 3.1.

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](#)" (page 88).

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 *Communication Server 1000 Fault Management—SNMP (NN43001-719)*.

Campus Redundancy

Contents

This section contains information on the following topics:

- "Description" (page 90)
 - "High Availability (HA) package enhancement" (page 91)
 - "High Speed Pipe (HSP) IP address management enhancement" (page 91)
 - "Stop and Copy protocol enhancement" (page 91)
- "Operating parameters" (page 92)
- "Normal Operations" (page 92)
 - "Warm start and Cold start" (page 93)
 - "Fault Detection" (page 94)
 - "Switchover" (page 94)
 - "Heartbeat" (page 97)
- "Network topology" (page 97)
 - "Switching Equipment" (page 99)
- "Call Server operation during IP network failure" (page 100)
 - "ELAN subnet connectivity between the CPUs is lost but HSP is still operational" (page 101)
 - "HSP connectivity is lost but ELAN subnet connectivity between the CPUs is operational" (page 101)
 - "ELAN subnet and HSP connectivity is lost between the CPUs" (page 101)
- "HSP configuration" (page 102)
 - "Initial installation" (page 102)
 - "HSP recommendations and rules" (page 102)
 - "High Speed Pipe IP address configuration" (page 103)
 - "Customer validation" (page 108)

- "IP Telephony node configuration" (page 108)
- "Upgrading a redundant system" (page 108)
- "Downgrading a redundant system" (page 110)
- "HSP maintenance" (page 111)
 - "STAT CPU" (page 111)
 - "STAT HSP" (page 113)
 - "STAT ELNK" (page 114)
- "Troubleshooting" (page 115)

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. The CS 1000E system allows campus mirroring to operate using other vendors' switching products in addition to the BayStack 470. See "[Third-party vendor switching equipment](#)" (page 100).

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 Systems.

The HSP is the interface 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 Availability (HA) package enhancement

The Campus Redundancy enhancements in Release 5.0 include the addition of the 410 HIGH_AVAIL HIGH AVAILABILITY package for CP PM servers. If the HA package is present in the keycode, the CP PM Call Server uses the HSP to detect the presence of the other core. If the other core is detected, both cores negotiate to determine which is the active core and which is the standby core. If the CP PM Call Server cannot detect the other core, it comes up as a single core system.

If the HA package is not present in the keycode, the existing Call Server software is modified to block the HSP connection so that the CP PM Call Server does not attempt to detect the presence of the core. In the absence of the HA package, the CP PM Call Server runs as a single core system, even in a system with two cores and the HSP ports on both cores are connected.

High Speed Pipe (HSP) IP address management enhancement

This 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.

With Release 5.0, Stop and Copy includes a checksum mechanism to ensure mirror imaging of data on both cores of a redundant system. The checksum mechanism does the following:

- ensures data validity in both cores
- protects data from corruption
- reduces the time and process of Stop and Copy, thereby reducing graceful switchover time by approximately 25%
- reduces graceful switchover failures

If the checksum does not match, protected data is copied as part of Stop and Copy.

Previously, a Stop and Copy failure during graceful switchover left duplicate IP addresses on the HSP (High Speed Pipe) link, causing a communication failure between active and inactive cores. To restore redundancy, the inactive core must be manually restarted. With Release 5.0, the system is restored to fully redundant mode after a failed Stop and Copy. When redundancy cannot be realized, the cores are split and the previously active core continues to be operational.

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](#)" (page 102) 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.

Warm start and Cold start

Warm start

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 (i.e. not reloaded from hard drive) and the task rebuilds all the unprotected data. In addition, established calls are rebuilt in the INITIALIZE procedure.

Cold start

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 is restarted 15 times, a system warm start is 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 triggers a system warm start. If the warm start process cannot reset the hardware watchdog, the second hardware watchdog triggers a system cold start.

Exception handling

When a processor exception occurs, the exception handler analyzes 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 warm start is invoked.

Health Monitoring

Each Call Server possesses a health count (available via the STAT HEALTH or STAT CPU command in overlay 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. The redundant CPU resumes 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 becomes the active side.

The previously active side invokes a warm start after the copying operation is completed. After the warm start, it becomes the redundant side.

During a graceful switchover, there is usually no impact to calls already in progress. There is a brief duration whereby new calls are not 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

When it is decided that the active side is inoperable (e.g. power or processor failure, watchdog timeout, exceptions), the redundant side warm starts and takes over control. The switchover does not occur immediately, because when 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. The following steps are required to provision this.

ATTENTION

IMPORTANT!

- 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.
- 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.
- 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.

- 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 for more information about the impact of switchover on calls, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)*.

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

Conference call survivability With Release 5.0, conference calls on the CS 1000E system are rebuilt after system initialization, including initialization due to an ungraceful switchover of cores. This restores all established calls involved in add-on conference on the CS 1000E using network control memory. Any periodic tones in the conference call are dropped. The operation of Meet-Me conference calls is not affected. If a call requires allocation of a Physical Terminal Number (PTN) and is unable to get one after Call Server restart, the call is dropped.

ACD Queue Call Recovery ACD Queue Call Recovery (ACDR) restores transient calls in ACD queues during CPP ungraceful switchover. Data for transient calls is mirrored on the inactive core and used to rebuild ACD queues after a system initialization resulting from an ungraceful switchover. A maximum of 1000 calls can be restored. If another system initialization is invoked (INI within INI) during system initialization, ACDR continues to restore calls. However, if another system initialization is invoked (INI within re-INI), ACDR aborts and an INI0112 message prints on the maintenance TTY.

During a Call Server warm start, the MSDL gets disabled and re-enabled and the MSDL300 message prints on the maintenance TTY. The D-channels are also disabled and re-enabled, dropping the transient calls. If an ACD call is not recovered before the MSDL300 message prints, queued calls with ringback treatment are dropped. If the queued calls are provided with RAN/MUSIC treatment, the calls are not dropped and can be recovered as these calls are already established.

Heartbeat

The two CPUs exchange heartbeats 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 warm starts to become active after a certain period of time.

By optimizing timeout and threshold parameters used in retries of the heartbeat mechanism, ungraceful switchover trigger time is reduced to less than 15 seconds with CS Release 5.0. The optimization in the timing leads to a change in the INI policy. When the active core warm starts, the inactive core also reboots, so no swapping of the cores takes place.

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 Release 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 [Figure 6 "Call Server and Signaling Server \(HSP and ELAN subnet\) separated with Layer 2 switching products" \(page 98\)](#), is still supported as the base offering. The Campus Redundancy enhancements starting in Release 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 Release 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 m) 550 m
- 1000BASE-SX on MultiMode Fiber (62.5 m) 275 m
- 1000BASE-LX on MultiMode Fiber (50 m) 550 m
- 1000BASE-LX on MultiMode Fiber (62.5 m) 550 m
- 1000BASE-LX on SingleMode (9 m) 5 km

- 1000BASE-XD on SingleMode (9 m) 40 km

Campus Redundancy Baystack 470 Bandwidth Use

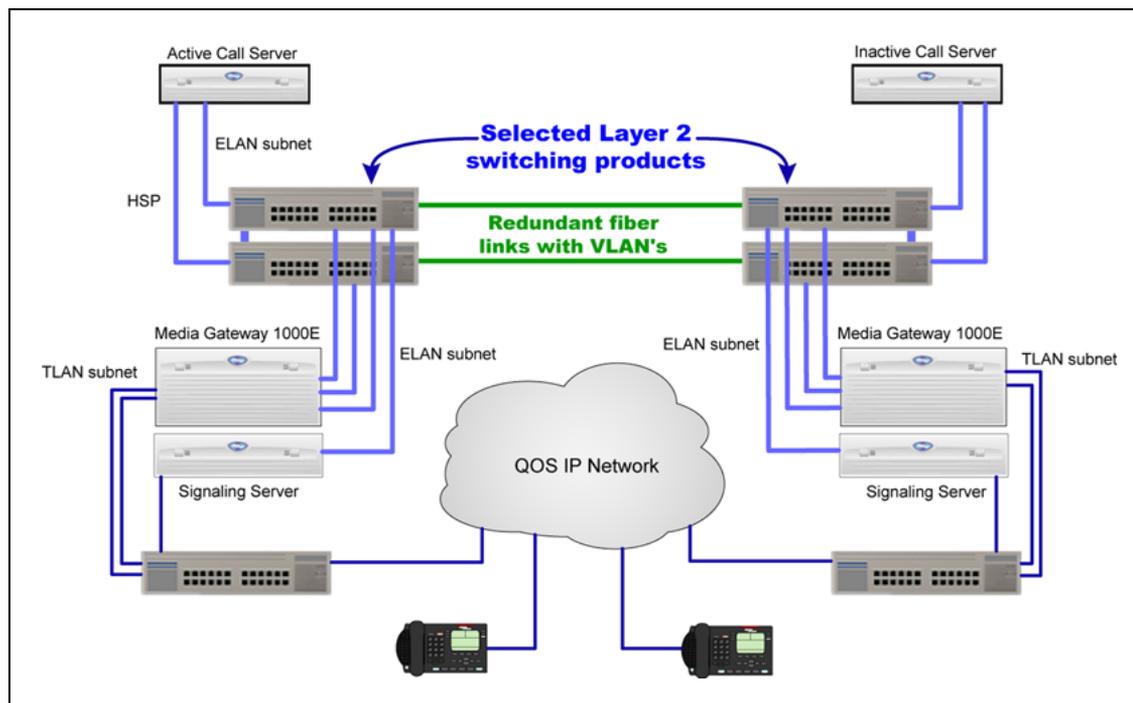
The Communication Server 1000E ELAN and HSP Ethernet links each require a dedicated 100 Mbps VLAN on the Baystack 470 1Gbps link. Although not specifically stated in the NTP's, the remainder of the Baystack 470 1Gbps Fiber link (800 Mbps) can be used for other data.

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 further ensures that the ELAN and HSP ports always have enough bandwidth to complete their tasks.

Figure 6
Call Server and Signaling Server (HSP and ELAN subnet) separated with Layer 2 switching products

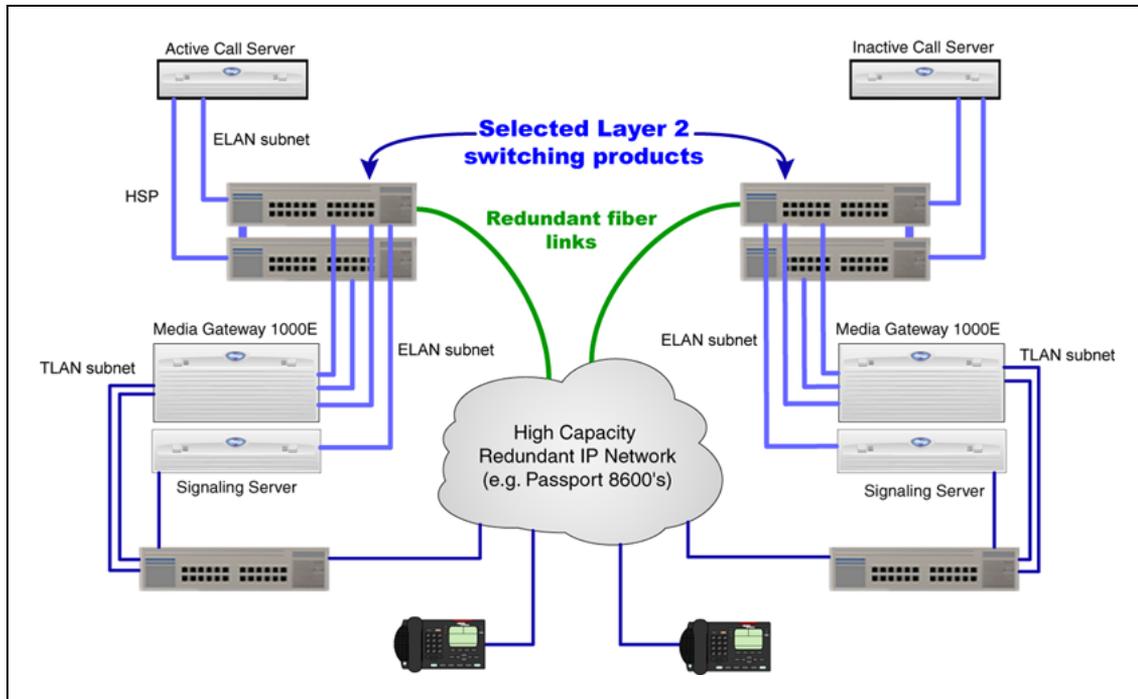


In addition, various other network topologies are supported that allow converged voice and data traffic to share the links between locations. However, the network design must include mechanisms such as priority,

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 7 "Call Server and Signaling Server (ELAN subnet and HSP) separated by high capacity network" (page 99) illustrates an alternative network topology that supports the Campus Mirroring of CS 1000E CPUs.

Figure 7
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 CAYALYST (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. When the HSP connection is restored then health information is exchanged. The CPU with the lower health count reboots 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" \(page 108\)](#).
- 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 1: The HSP IP addresses and subnet mask are not activated until the SET HSP_IP command is used or the CPU reboots.

Note 2: 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 HostnameIP Address

1 LOCAL_PPP_IF137.135.192.4

2 REMOTE_PPP_IF100.1.1.1

3 ACTIVE_CPU47.11.226.10

4 INACTIVE_CPU47.11.226.11

7 DEV_SIDE0_HSP192.168.100.10

8 DEV_SIDE1_HSP192.168.100.11

=> 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 9 "LD 117 HSP subnet mask commands" (page 106) describes the LD 117 HSP subnet mask commands.

Table 9
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
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 10
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. Because 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 11
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: 0xfffff00; Subnetmask: 0xfffff00

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](#)" (page 102).
- 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 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](#)" (page 91).

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 12 "Example of upgrading system software" (page 109) gives an example of upgrading a redundant system from CS 1000 Release 4.0 software to Release 4.5 software.

Table 12
Example of upgrading system software

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
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

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

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 HostnameIP Address

1 LOCAL_PPP_IF137.135.192.4

2 REMOTE_PPP_IF100.1.1.1

3 ACTIVE_CPU47.11.226.10

```

4 INACTIVE_CPU 47.11.226.11
7 DEV_SIDE0_HSP192.168.100.10
8 DEV_SIDE1_HSP192.168.100.11
=> 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 memory 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 goes down.

Table 13
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>

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

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: 0xfffff00; Subnetmask: 0xfffff00

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: 0xfffffe0

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 is 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" (page 117)

"BayStack 470-24T configuration" (page 119)

Description

Table 14 "BayStack 470-24T VLAN assignment" (page 117), Table 15 "VLAN port configuration" (page 118), and Table 16 "MultiLink Trunk configuration" (page 119) describe the configuration of the BayStack 470-24T VLANs.

Table 14
BayStack 470-24T VLAN assignment

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)

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 15
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
Switch 2	1-24	3	No
	25-26	1	Yes

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

Table 16
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 18 "Configuring the BayStack 470-24T using Web-based management" (page 119) must be performed for the switch stacks at both Call Server sites.

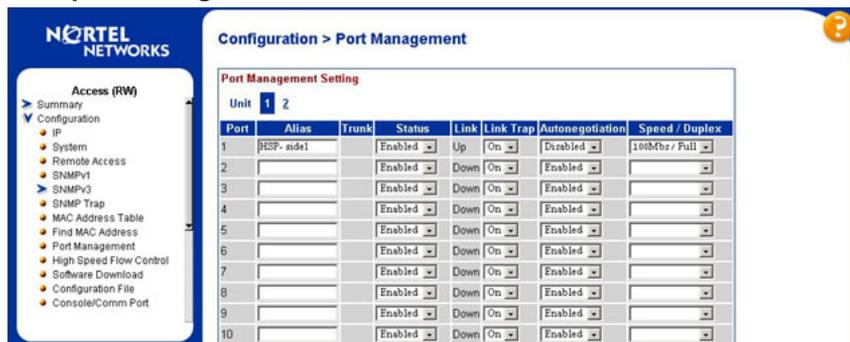
Procedure 18

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

Step	Action
------	--------

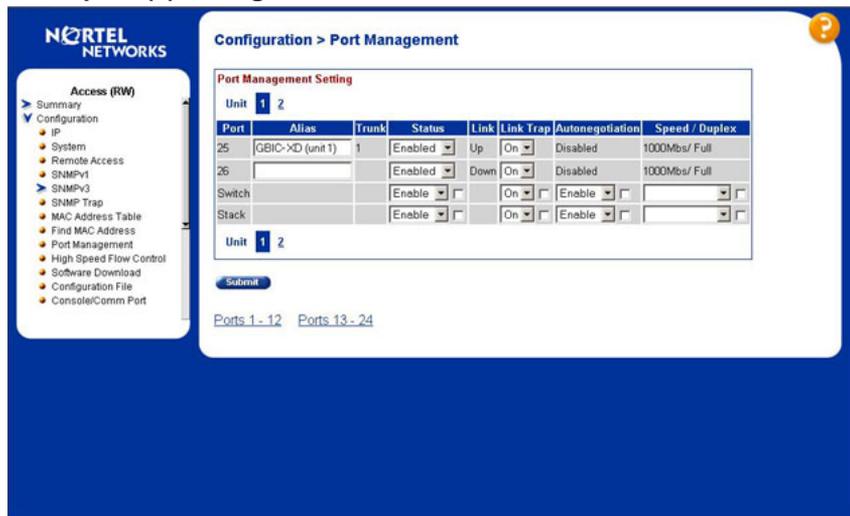
- | | |
|---|--|
| 1 | From the main menu of the BayStack 470-24T Web-based management interface, choose Configuration > Port Management . |
| 2 | Configure the HSP network interface on switch 1 (and 3) as shown in Figure 8 "HSP port configuration" (page 120) . |

Figure 8
HSP port configuration



- 3 Configure the GBIC network interface on switch 1 (and 3) as shown in Figure 9 "GBIC port (1) configuration" (page 120).

Figure 9
GBIC port (1) configuration



- 4 Configure the Call Server ELAN network interface on switch 2 (and 4) as shown in Figure 10 "Call Server ELAN port configuration" (page 121).

Figure 10
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	<input type="checkbox"/>	On	Enable	<input type="checkbox"/>
Stack			Enable	<input type="checkbox"/>	On	Enable	<input type="checkbox"/>

Unit 1 2

Submit

- 5 Configure the GBIC network interface for switch 2 (and 4) as shown in Figure 11 "GBIC port (2) configuration" (page 121).

Figure 11
GBIC port (2) configuration

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	<input type="checkbox"/>	On	Enable	<input type="checkbox"/>
Stack			Enable	<input type="checkbox"/>	On	Enable	<input type="checkbox"/>

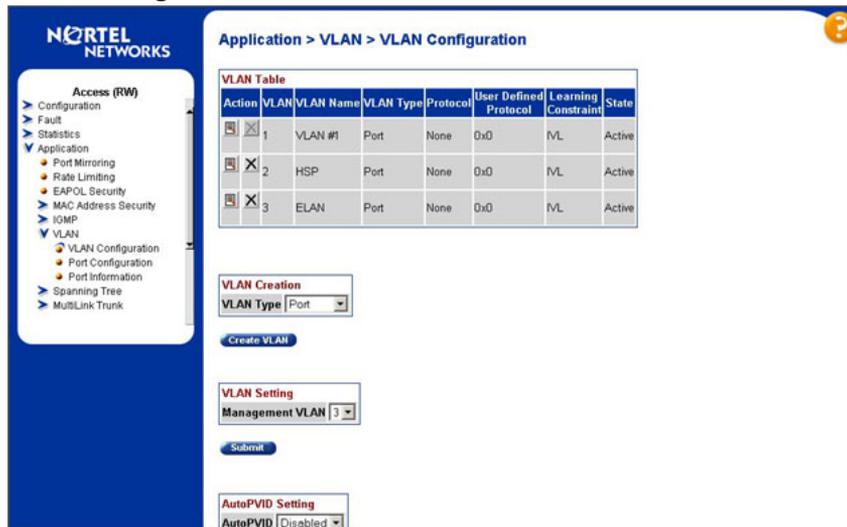
Unit 1 2

Submit

Ports 1 - 12 Ports 13 - 24

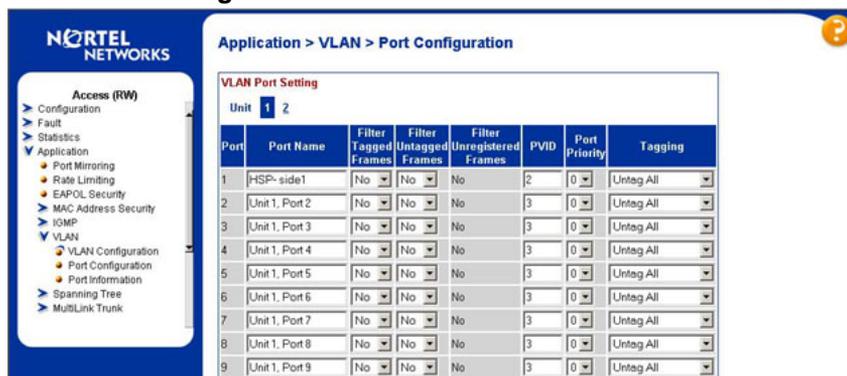
- 6 From the main menu, choose **Application > VLAN > VLAN Configuration**.
- 7 Configure the VLANs as shown in Figure 12 "VLAN configuration" (page 122).

Figure 12
VLAN configuration



- 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 13 "HSP VLAN configuration"](#) (page 122).

Figure 13
HSP VLAN configuration



- 10 Configure the GBIC VLAN network interfaces for switch 1 (and 3) as shown in [Figure 14 "GBIC \(1\) VLAN configuration"](#) (page 123).

Figure 14
GBIC (1) 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 1	No	No	No	1	0	Tag All
26	Unit 1, Port 26	No	No	No	1	0	Tag All

Unit 1 2

Submit

Ports 1 - 12 Ports 13 - 24

- 11 Configure Call Server ELAN VLAN network interface on switch 2 (and 4) as shown in Figure 15 "Call Server ELAN VLAN configuration" (page 123).

Figure 15
Call Server ELAN VLAN configuration

Application > VLAN > Port Configuration

VLAN Port Setting

Unit 1 2

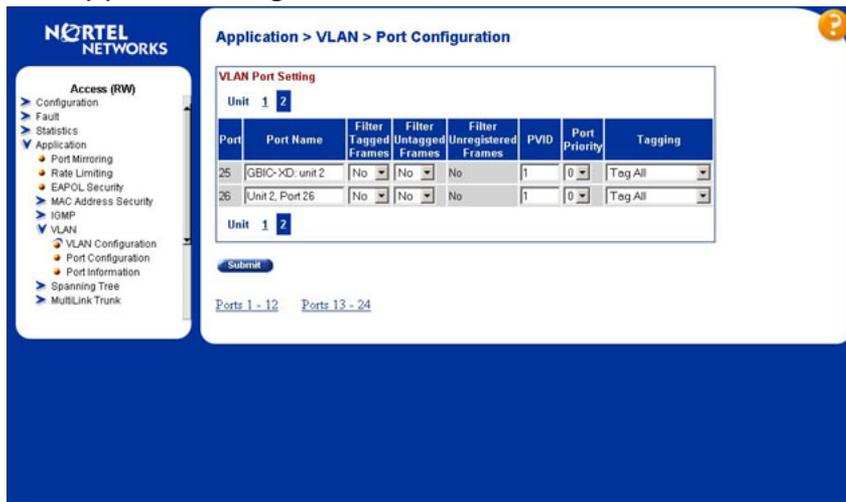
Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
13	Unit 2, Port 13	No	No	No	3	0	Untag All
14	Unit 2, Port 14	No	No	No	3	0	Untag All
15	Unit 2, Port 15	No	No	No	3	0	Untag All
16	Unit 2, Port 16	No	No	No	3	0	Untag All
17	Unit 2, Port 17	No	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 16 "GBIC (2) VLAN configuration" (page 124).

Figure 16
GBIC (2) VLAN configuration



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

The **VLAN Configuration** Web page appears. For more information, see [Figure 12 "VLAN configuration"](#) (page 122).

- 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 17 "VLAN port membership configuration"](#) (page 125).

Figure 17
VLAN port membership configuration

The screenshot shows the 'VLAN Configuration: Port Based' page for VLAN 1. The 'VLAN Name' is 'VLAN #1'. The 'Learning Constraint' is 'VL'. The 'Port Membership' table shows that all 24 ports in Unit 1 and Unit 2 are checked for membership.

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 checked="" type="checkbox"/>																								
Unit 2	<input checked="" type="checkbox"/>																								

- 17 Configure HSP VLAN port membership as shown in Figure 18 "HSP VLAN port membership configuration" (page 125).

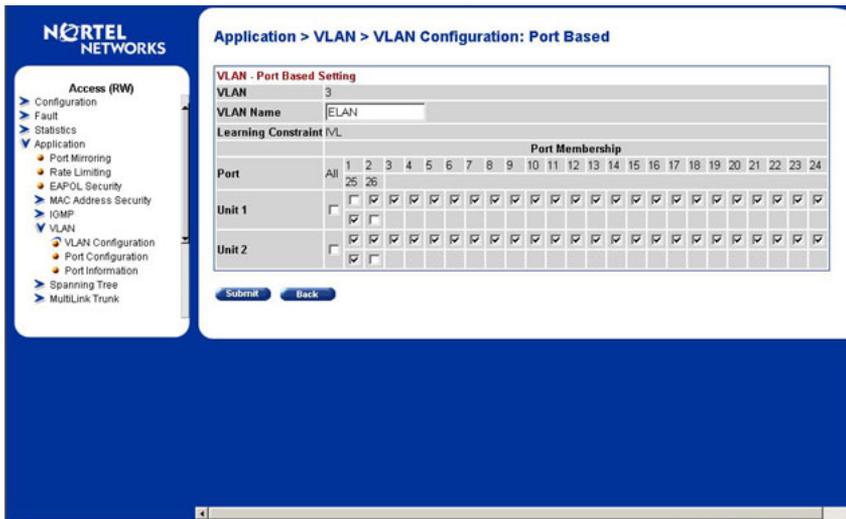
Figure 18
HSP VLAN port membership configuration

The screenshot shows the 'VLAN Configuration: Port Based' page for VLAN 2. The 'VLAN Name' is 'HSP'. The 'Learning Constraint' is 'VL'. The 'Port Membership' table shows that all 24 ports in Unit 1 and Unit 2 are checked for membership.

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 checked="" type="checkbox"/>																								
Unit 2	<input checked="" type="checkbox"/>																								

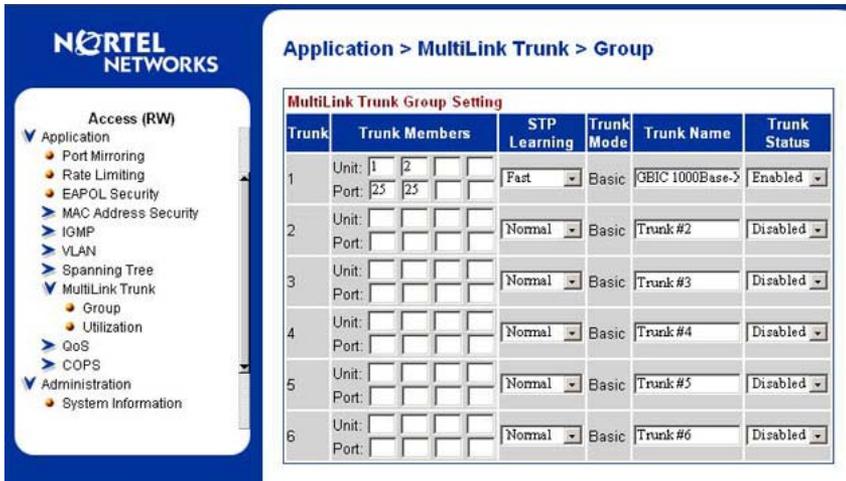
- 18 Configure ELAN VLAN port membership as shown in Figure 19 "ELAN VLAN port membership configuration" (page 126).

Figure 19
ELAN VLAN port membership configuration



- From the main menu, choose **Application > MultiLink Trunk > Group**. Configure the MultiLink Trunk Group settings as shown in Figure 20 "MultiLink Trunk Group settings configuration" (page 126).

Figure 20
MultiLink Trunk Group settings configuration



—End—

Appendix B

Controlled Load-sharing zones

Contents

This section contains information on the following topics:

"Network bandwidth management zones" (page 127)

"Configuring zone parameters at the backup site" (page 129)

"Configuring zone parameters at the home site" (page 135)

"Configuring zone-based digit manipulation" (page 139)

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 Reference (NN43001-283)*.

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 about system configuration, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*. Also refer to *Communication Server 1000E Installation and Commissioning (NN43041-310)* or *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning (NN43021-310)* 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" \(page 129\)](#)
2. ["Configuring zone parameters at the home site" \(page 135\)](#)
3. ["Configuring zone-based digit manipulation" \(page 139\)](#)

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 Commissioning (NN43001-313)*.

Zone parameters are defined at the backup system in LD 117 ([Procedure 20 "Configuring the home system zone" \(page 135\)](#)). 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.

**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.

Procedure 19**Configuring ESN and redundant IP Phone zones****Step Action**

- 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 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

- 3 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 Commissioning (NN43001-313)*.

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.

ATTENTION**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

Command	Description
<pre>NEW_ZONE <xxx> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType>]</pre>	<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
<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>	

Command	Description
	<p>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:</p> <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
<p>Note 1: If the Network Bandwidth Management feature is going to be used, the <code>intraZoneBandwidth</code> and <code>interZoneBandwidth</code> 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 <code>intraZoneStrategy</code> and <code>interZoneStrategy</code> 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 Commissioning (NN43001-313)*.

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>.

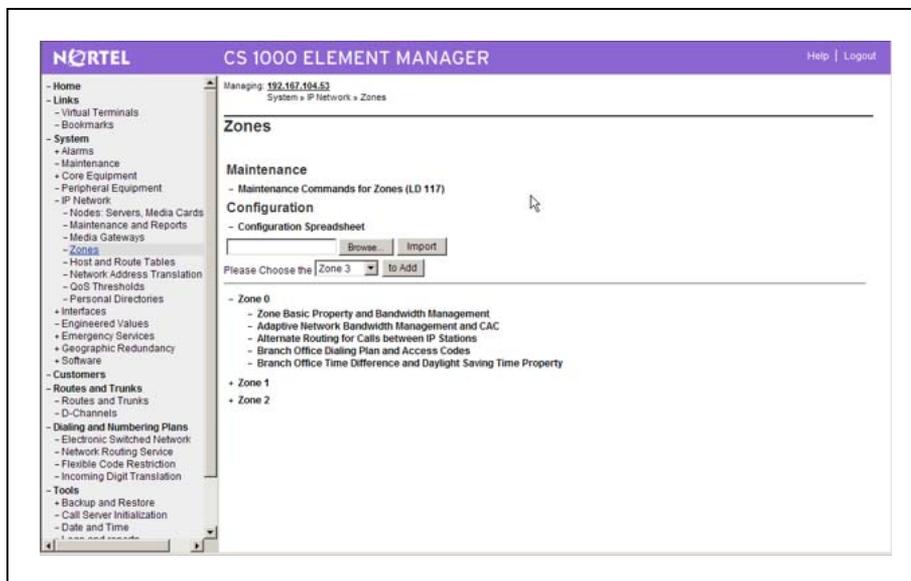
—End—

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 21 "Zone configuration on the backup system"](#) (page 134) is the main window used for zone configuration in Element Manager. Select **System > IP Network > Zones** from the Element Manager navigator to open this window.

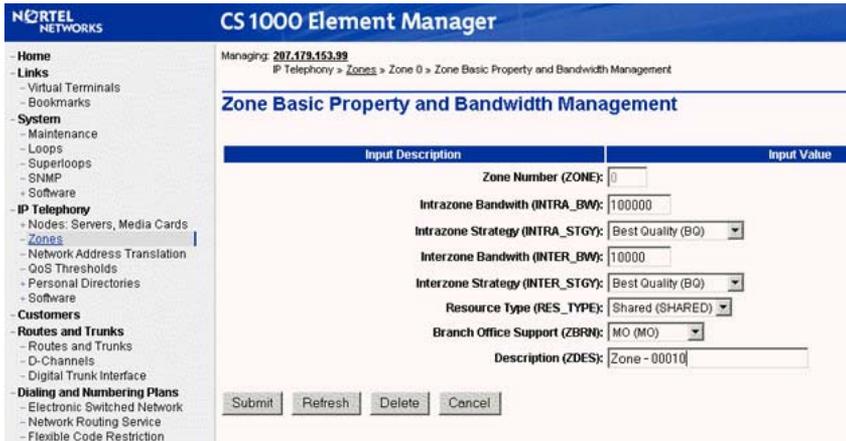
Figure 21
Zone configuration on the backup system



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

- Basic Property and Bandwidth Management (see [Figure 22 "Zone Basic Property and Bandwidth Management"](#) (page 135))
- 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 22
Zone Basic Property and Bandwidth Management



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.



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.

Procedure 20

Configuring the home system zone

Step	Action
------	--------

- | | |
|---|--|
| 1 | Set the current date and time. See <i>Software Input/Output Administration (NN43001-611)</i> . |
|---|--|

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.

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
- - 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 23 "Zone Basic Property and Bandwidth Management"](#) (page 138). 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.

ATTENTION

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 is not 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

Command	Description
	<p>— 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:</p> <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—

Element Manager zone configuration on the home system

Figure 23 "Zone Basic Property and Bandwidth Management" (page 138) shows the only zone configuration screen required on the home system. It is an alternative to zone configuration using LD 117.

Figure 23
Zone Basic Property and Bandwidth Management

The screenshot shows the CS 1000 Element Manager web interface. The main title is 'CS 1000 Element Manager'. Below the title, it says 'Managing: 207.179.153.99' and 'IP Telephony > Zones > Zone 0 > Zone Basic Property and Bandwidth Management'. The page title is 'Zone Basic Property and Bandwidth Management'. The configuration area has a table with two columns: 'Input Description' and 'Input Value'. The inputs are:

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 configuration area, 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 Commissioning (NN43001-313)* 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 Commissioning (NN43001-313)* for more details.

Procedure 21

Configuring the zone-based digit manipulation

Step	Action
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 "2 101 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 Commissioning (NN43001-313)*.

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](#)) 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 are not 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—

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 are configured with local numbers, such as 555-1212 or 967-1111.

Table 17 "Example dialing string, area codes, and Access Codes" (page 142) uses the following configuration at the backup system for home system telephones to reach the PSTN.

Table 17
Example dialing string, area codes, and Access Codes

	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".
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 Fundamentals

Copyright © 2004-2007, Nortel Networks
All Rights Reserved.

Publication: NN43001-507
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

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

Sourced 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, the Nortel Logo, the Globemark, SL-1, Meridian1, and Succession are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

