Nortel Communication Server 1000

New in this Release

NN43001-115

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

Sourced in Canada.

Revision history

May 2007
Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0.

Contents

How to get help 11
Getting help from the Nortel Web site 11
Getting help over the telephone from a Nortel Solutions Center 11
Getting help from a specialist by using an Express Routing Code 11
Getting help through a Nortel distributor or reseller 12

Introduction 13
Subject 13
Applicable Systems 13
Communication Server 1000 and Meridian 1 Release 5.0 database conversion 14
Conventions 14
Terminology 14

Overview 15
New Systems 15
Key Attributes 16
Key Features 17
Features described only in this document 17

Simplicity 19

Common Processor Pentium Mobile Call Server 21

Signaling Server 23
Nortel Common Processor Pentium Mobile server 24
International Business Machines X306m server 24
Hewlett Packard DL320-G4 server 25

Media Gateway Controller 27
Introduction 27
Features and enhancements 27
Hardware description 28
Conference capacity 29
Media security feature 30
For more information 30

DSP Daughterboard 31
Introduction 31

Configuration and maintenance 31
For more information 31

MC32S Media Card 33

Resiliency 35

Geography Redundancy: Survivable Media Gateway 37
Description 37

Network Wide Redundancy Phase II 39
Feature Description 39
Temporary IP User license 39

CPP Redundancy and Resiliency Phase II 41

Diagnostic and Fault Reporting Enhancements 45
Diagnostic enhancements 45
Fault reporting enhancements 46

SNMP Enhancements 47
Description 47
Enhancements 47
Single point of configuration 47
Common Trap MIB 48
Configurable Trap community string 48
Network routing table entries 48
MIB II System group 48
SNMP support for Linux systems 48
SNMP support for new hardware 49

VTRK Failover Upon Network Failure 51
Overview 51
Description 51
Administration and maintenance 53
Element Manager configuration 53
VTRK Network Health Monitor configuration for an IP Telephony node 53
VTRK Network Health Monitor Configuration CLI commands 56
New SNMP alarms 56

Open Interoperability 59

Network Routing Service on Linux 61
Network Routing Service 61
SIP Proxy 61
NRS database 62
NRS Manager 62

Dual Tone Multi-frequency (DTMF) Handling using RFC2833 63
Set payload type 64

Network Time Protocol **67**
Feature description 67
Time distribution across the network 67
NTP Server 67
Mode of communication 67
NTP threshold levels 68
Secure mode of operation 68
Time zone 68
Daylight-Saving Time 68
Mode of synchronization 68
NTP status 69
Print NTP parameters 69
Feature interactions 70
Network Time Synchronization 70
Geographic Redundancy 70
Call Detail Recording 70
Traffic Analysis 70
Call accounting/call tracking 70
Manual time updates using LD 02 70
Attendant Console Time and Date key 71
Feature implementation using LD 117 71
Prerequisites for implementing NTP using LD 117 71
Procedures for implementing NTP using LD 117 71
Configuring primary NTP server address 73
Configuring secondary NTP server IP address (optional) 73
Changing communication mode: Call Server to NTP server over ELAN subnet 74
Changing communication mode: Call Server to NTP server using Signaling Server 74
Configuring NTP threshold levels 75
Configuring NTP Time interval 75
Configuring secure mode of operation 76
Enabling secure mode of operation 77
Disabling secure mode of operation 77
Configuring UTC offset for local time zone 78
Adjusting for Daylight Saving Time 78
Enabling NTP 78
Disabling NTP 79
Synchronizing NTP to run in the background 79
Synchronizing NTP manually 80
Stopping background synchronization 80
Checking NTP status 81
Printing NTP parameters 81

Feature implementation using Element Manager 81
Prerequisites for implementing NTP using Element Manager 81
Procedures for implementing NTP using Element Manager 82
Procedures for implementing NTP using EM 82
Configuring NTP parameters using EM 83
Adjusting for Daylight saving using EM 84
Enabling NTP using Element Manager 84
Disabling NTP using Element Manager 85
Synchronizing NTP manually using Element Manager 85

Nortel Converged Office 87

Security and Emergency Services 89

Security Enhancements 91
Overview 91
OAM security enhancements 91
Improved account management 91
Improved logging 92
Enhanced remote access security through SSH 92
Media Security 92
Intrasystem Signaling Security 93
Transport Layer Security for SIP 93
Secure signaling using SMC 2450 93
For more information 94

Emergency Services Access 95
Emergency Services Networked M911 Operation 96
Basic Emergency Services When VO Logged Out 97

Business Continuity 99

IP Line 5.0 feature enhancements 101
Description 101
New IP Phone Types 101
New languages and Unicode support 104
Expansion Module for IP Phone 1100 Series font support 105
Downloading and configuring fonts 105
IP Client cookies 107
Live Dialpad 108

Context-sensitive soft keys 109
Feature description 109
Soft keys configuration 109
Operating parameters 111
Feature restrictions 112
Feature interactions 112

Feature packaging 112
Feature implementation 112
Feature operation 113
Using call features 114
CallPilot voice-mailbox-related soft keys 116

CLID Name Enhancement 119
Feature description 119
Feature restrictions 120
Sample Scenarios 121
Operating Parameters 127
Privacy and security 128
Error handling 129
Feature interactions 129
Call transfer 129
Call forward all calls, hunt, no answer, and busy 130
Connected number 130
Calling party name display 130
Network call redirection 130
Numbering plan interactions 131
Trunks involved 131
Feature packaging 131
Feature implementation 131
Implementation using overlays 131
Implementation using Element Manager 133

ISDN CLID Enhancement 139
Feature description 139
Feature restrictions 140
Sample scenarios 141
Feature interactions 149
CDR: Abandon record (B) 149
Display 149
ACD 149
Calling Party Name Display 150
Administration from an Attendant Console 150
Feature packaging 150
Feature implementation 150
Implementation using overlays 150
Implementation using Element Manager 153

Bandwidth Management Support for Network Wide Virtual Office 155

Network Music 157
Description 157

Feature operation 157
Network Music Agent 157
Music broadcast 158

System Management 159

Element Manager Enhancements 161
Emergency Services 161
Phones 161
Customers 162

Telephony Manager 163
Introduction 163
New and enhanced applications 163
Telephone Manager (Web Station) enhancements 163
Web maintenance enhancements 164
Alarm management enhancements 164
Alarm notification enhancements 165
Traffic analysis enhancements 165
Additional enhancements 165

Global Address Book Synchronization 167

Enterprise Common Manager 169
Enterprise Common Manager overview 169
Key benefits and features 170
Security domain 170
Certificate management 171
Secure shell trust of CA 171
Security framework 171
Access control policies 172

How to get help

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

Getting help from the Nortel Web site

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

www.nortel.com/support

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

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

Getting help over the telephone from a Nortel Solutions Center

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

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

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

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.

Introduction

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

Subject

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

www.nortel.com

Applicable Systems

This document applies to the following systems:

- CS 1000E CP PII
- CS 1000E CP PIV
- CS 1000E CP PM HA (Chassis)
- CS 1000E CP PM HA (Cabinet)
- CS 1000E CP PM SA (Chassis)
- CS 1000E CP PM SA (Cabinet)
- CS 1000M Single Group CP PII (AC/DC)
- CS 1000M Multi Group CP PII (AC/DC)
- CS 1000M Single Group CP PIV (AC/DC)
- CS 1000M Multi Group CP PIV (AC/DC)

Communication Server 1000 and Meridian 1 Release 5.0 database conversion

Automatic Call Server database conversion is supported for all Succession and Communication Server (CS) 1000 releases and for Meridian 1 Release 23 or later.

Database upgrades for software releases prior to Meridian 1 Release 23 require a Nortel In-House Conversion (IHC), a database retype, or upgrade in a Distributor's lab (if already equipped with required hardware and software). Direct conversion in the field is not supported for any release prior to Release 23. The (IHC) service is available to convert any database to CS 1000 Release 5.0 and eliminates the need for intermediate hardware and software. The conversion of the customer's source database is done in Nortel's Enterprise Software Solutions lab.

Conventions

Terminology

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

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

The following systems are referred to generically as "Small System":

- Meridian 1 Option 11C Chassis
- Meridian 1 Option 11C Cabinet

The following systems are referred to generically as "Large System":

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 Option 61C
- Meridian 1 Option 81C

Overview

Communication Server (CS) 1000 Release 5.0 is the latest release for the CS 1000 family of products. Building on CS 1000 Release 4.5, CS 1000 Release 5.0 is an evolution of the traditional TDM enterprise network to a converged IP based network.

The CS 1000 Release 5.0 is a reliable and secure platform for VoIP communications and is designed to be a more open and simplified platform, which speeds deployment and improves manageability.

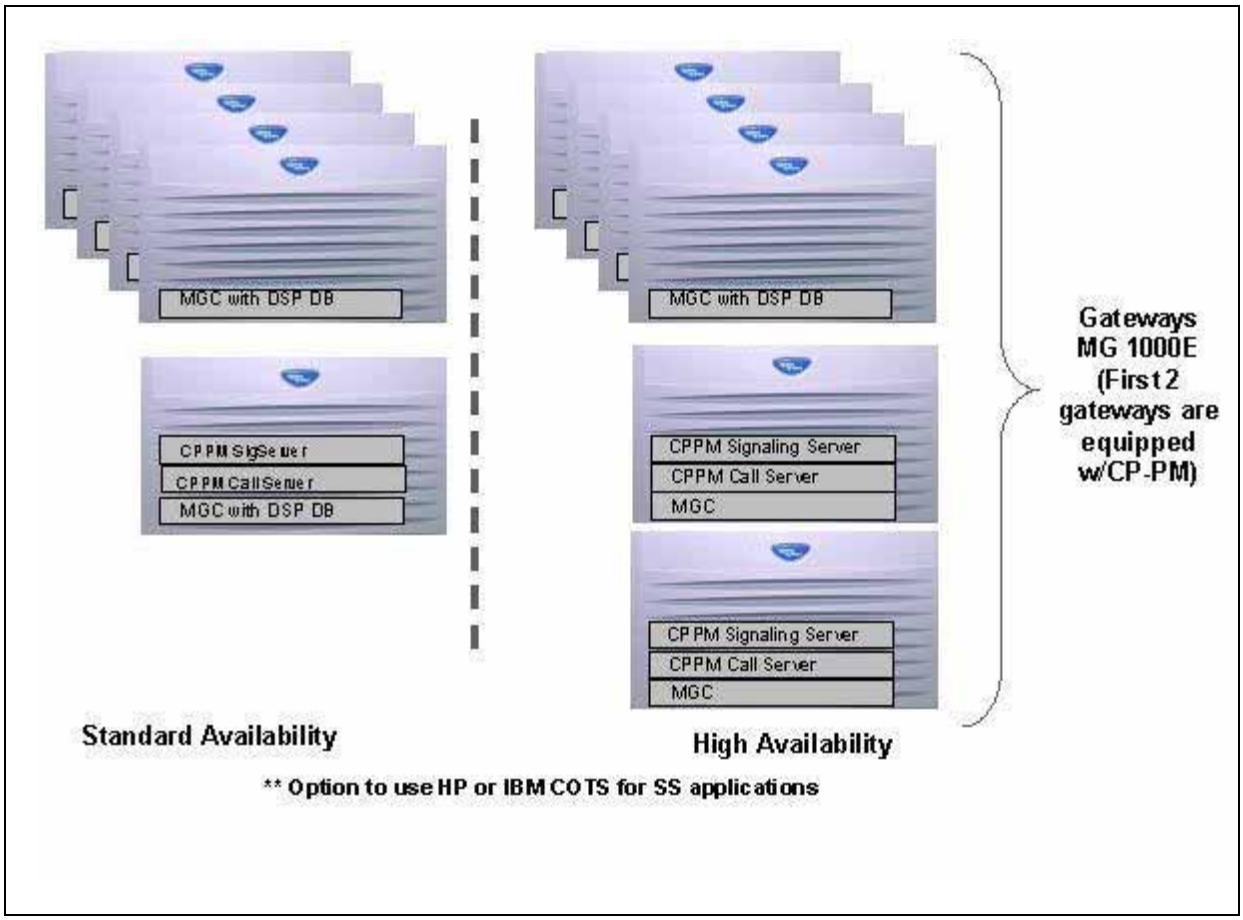
New Systems

CS 1000 Release 4.0 platform was introduced with redundant CP Pentium II/ IV processors. This platform provided redundancy and scalability required for larger line size customers, while the CS 1000S and CS 1000M Cabinet and Chassis provided a more cost effective solution for the small to mid-size customer.

CS 1000 Release 5.0 introduces a modification to the CS 1000E architecture that offers options for single and redundant processors, an option for the processor type and customer choice in form factor for the Media Gateway. With CS 1000 Release 5.0, a customer can deploy existing or new cabinets or chassis' as Media Gateway 1000 (MG 1000). A new Call Processor platform (CP PM) is available which occupies a slot in a MG 1000 Cabinet or Chassis. This new processor can be deployed as a single call processor (Standard Availability CS 1000E) or in a redundant processor configuration (High Availability CS 1000E). The redundant CP PIV processor configuration is also still available as a High Availability CS 1000E system. Each Media Gateway is controlled by a new Media Gateway Controller (MGC) that can support up to 128 DSP channels installed as daughterboards on the MGC. .

The CS 1000E Standard Availability replaces CS 1000S, CS 1000M Chassis, and CS 1000M Cabinet system types. The Standard Availability (SA) system can be upgraded to a High Availability (HA) system with the addition of a second CP PM Call Server and by enabling the HA software package.

Figure 1
Standard Availability CS 1000E and High Availability CS1000E



CS1000E Release 5.0 supports the following capacity increases:

- Number of IP Phones supported increases from 15,000 to 22,500 phones
- Number of supported Media Gateways increases from 30 to 50

There are also new Signaling Server platforms available. The customer has the choice of using the new CP PM as a Signaling Server installed in a Media Gateway Chassis or Cabinet (or in a UEM for a CS 1000M SG/ MG) or using an IBM or HP 1U COTS (Commercial off-the-shelf) server.

Key Attributes

- **Adaptable to meet current and future needs**
  - — Delivers investment protection and evolution path to next-generation multimedia communications

- **Superior IP Telephony experience**
  - — More open platform to take advantage of innovative applications, and feature-rich next generation clients
- **Improved reliability and security**
  - — Business continuity improvement from a reliable and secure environment
- **Simplified convergence solution**
  - — Product portfolio simplified for easier deployment, configuration and management

Key Features

CS 1000 Release 5.0 delivers significant new features and capabilities in a more resilient, secure, simple and open call server solution.

In this document, the new features and hardware in CS 1000 Release 5.0 are divided under the headings:

- "Simplicity" (page 19)
- "Resiliency" (page 35)
- "Open Interoperability" (page 59)
- "Security and Emergency Services" (page 89)
- "Business Continuity" (page 99)
- "System Management" (page 159)

Features described only in this document

The description, and associated procedures for the following features are described only within this document:

- "CLID Name Enhancement" (page 119)
- "Context-sensitive soft keys" (page 109)
- "Dual Tone Multi-frequency (DTMF) Handling using RFC2833" (page 63)
- "ISDN CLID Enhancement" (page 139)
- "Network Time Protocol" (page 67)

Simplicity

Communication Server (CS) 1000 Release 5.0 introduces new hardware components that represent a significant change to the architecture of the CS 1000 portfolio. With the new architecture, CS 1000 Media Gateways (MG 1000) can be either a Cabinet or Chassis form factor for a Media Gateway Contoller. A system now scales from the smallest to the largest line size and can have either a single or redundant call processor with the same continuously scalable architecture.

CS 1000 Release 5.0 reduces the number and type of gateways and Call Servers required to support services and users. Benefits include less complexity, greater scalability (from 50 to 22,500 users), greater integration, and fewer individual systems.

The following is a summary of the new hardware components and corresponding applications:

- CP PM - Common Processor Pentium Mobile (NTDW61BAE5); can be configured to run as Call Server or Signaling Server.
- MGC – Media Gateway Controller (NTDW60BAE5) runs as a MG1000E controller and replaces the gateway controller functionality of the existing Small System Controller (SSC) (NTDK20).
- DSPDB-32 – DSP Daughterboard 32-port (NTDW62AAE5) is a 32-port DSP daughterboard that is plugged into a slot on the MGC.
- DSPDB-96 – DSP Daughterboard 96-port (NTDW64AAE5) is a 96-port DSP daughterboard that is plugged into a slot on the MGC.
- MC32S – Media Card 32 Port Security; this is a media card with 32 DSP ports that replaces the existing Voice Gateway Media Card 32-port media card.
- COTS 1U Server – Commercial off the shelf server in a 1U form factor that can be used for Signaling Server or Network Routing Service (NRS). The CS 1000 Linux base operating system provides a Linux server platform for applications on a COTS Pentium server.

Common Processor Pentium Mobile Call Server

The Common Processor Pentium Mobile (CP PM) is a high-performance server that can act as either a Call Server or a Signaling Server in a Communication Server 1000E (CS 1000E) system.

There are two CP PM types available for CS 1000 Release 5.0: NTDW61BA and NTDW66AAE5. The NTDW61BA is used in the MG 1000E as either a Call Server or a Signaling Server, while the NTDW66AAE5 is used strictly as a Signaling Server in the CS 1000M SG or CS 1000M MG.

The CP PM Call Server delivers capacity improvements by providing flexible scaling of the CS 1000E from 0 to 22,500 sets. CS 1000 Release 5.0 also introduces a modification to the CS 1000E architecture that allows for:

- a Single processor (Standard Availability)
- redundant processors (High Availability)
- an option for the processor type
- customer choice in form factor for the Media Gateway

The CP PM can be deployed as a single call processor (Standard Availability CS 1000E) or in a redundant processor configuration (High Availability CS 1000E).

For more information about the CP PM Call Server, refer to *Circuit Card Reference (NN43001-311)*.

Signaling Server

The Signaling Server provides a central processor to drive Session Initiation Protocol (SIP) and H.323 signaling, IP Phone signaling, and IP Peer Networking, in CS 1000E and CS 1000M systems. The Signaling Server has both an ELAN and a TLAN network interface, and communicates with the Call Server through the ELAN subnet.

The Signaling Server provides signaling interfaces to the IP network using the following software components that run on the VxWorks™ real-time operating system:

- IP Phone Terminal Proxy Server
- SIP and H.323 signaling gateway (Virtual Trunk)
- Network Routing Service (NRS)
- CS 1000 Element Manager Web server
- IP Phone Application Server (Personal Directory, Callers List, and Redial List)

You can install Signaling Servers in your CS 1000 system in a load-sharing redundant configuration, for higher scalability and reliability.

CS 1000 Release 5.0 introduces three new servers that can host CS 1000 Release 5.0 applications:

- "Nortel Common Processor Pentium Mobile server" (page 24)
- "International Business Machines X306m server" (page 24)
- "Hewlett Packard DL320-G4 server" (page 25)

The legacy Nortel ISP1100 Signalling Server can still be used to host CS 1000 Release 5.0 software.

Nortel Common Processor Pentium Mobile server

The Nortel Common Processor Pentium Mobile (CP PM) server is a high-performance, circuit card-based server that can be configured as a Call Server or a Signaling Server in a CS 1000 Release 5.0 system. Two models are available:

- NTDW61BAE5 – can be configured as a Call Server or Signaling Server in a CS 1000E system
- NTDW66AAE5 – can be configured only as a Signaling Server in a CS 1000M system

Configured as a Signaling Server, the NTDW61BAE5 model is installed in a Media Gateway Chassis or Cabinet (MG 1000E) in a CS 1000E system. The NTDW66AAE5 model is installed in a Universal Equipment Module (UEM) in a CS 1000M SG or CS 1000M MG system.

The Nortel CP PM server has the following components:

- Intel Pentium M processor (1.4 Ghz)
- internal hard drive
- hot-pluggable Compact Flash (CF) card slot in the faceplate
- 2 Gb of SDRAM
- One 1 Gb/s Ethernet port
- Two 100BaseT Ethernet ports
- Two serial ports
- One USB port

For more information about installing and configuring the Nortel CP PM server as a Signaling Server, see *Signaling Server Installation and Commissioning (NN43001-312)*.

International Business Machines X306m server

The International Business Machines (IBM) X306m 1U server is a rack-mounted, Pentium 4, PC-based, industry-standard, commercial off-the-shelf (COTS) server.

The IBM X306m 1U server has the following components:

- Intel Pentium 4 processor (3.6 GHz)
- Two 80 GB simple swap Serial ATA hard drives (1 drive configured)
- 8 GB of RAM PC4200 DDR II by means of 4 DIMM slots (2 GB configured)
- Two 1 Gb/s Ethernet ports

- One DVD-COMBO (DVD/CD-RW) drive
- One serial port
- Four USB ports

For more information about the server, refer to the IBM xSeries 306m Types 8848 and 8491 User Guide shipped with the server.

For more information about installing and configuring the IBM X306m server as a Signaling Server, see *Signaling Server Installation and Commissioning (NN43001-312)*.

Hewlett Packard DL320-G4 server

The Hewlett Packard (HP) DL320-G4 1U server is a rack-mounted, Pentium 4, PC-based, industry-standard, commercial off-the-shelf (COTS) server.

The HP DL320-G4 1U server has the following components:

- Intel Pentium 4 processor (3.6 GHz)
- Two 80 GB SATA Hard drives (1 configured)
- 4 GB PC2-4200 ECC DDR2 SDRAM (2 GB configured)
- Two 10/100/1000BaseT Ethernet ports
- One CD-R/DVD ROM drive
- One serial port
- Three USB ports

For more information about the server, refer to the HP ProLiant DL320 Generation 4 Server User Guide shipped with the server.

For more information about installing and configuring the HP DL320-G4 server as a Signaling Server, see *Signaling Server Installation and Commissioning (NN43001-312)*.

Media Gateway Controller

Introduction

The Media Gateway Controller (MGC) card occupies the system controller slot 0 in the Media Gateway Chassis.

The NTDW60 MGC card provides a gateway controller for Media Gateways in a CS 1000E system. The MGC functions as a gateway controller under control of a CS 1000E (CP PII, CP PIV or CP PM) Call Server.

The MGC supports up to 128 DSP channels (equivalent of four Voice Gateway Media Cards) with the two expansion sites to accommodate Digital Signal Processor daughterboards (DSP DB). The 96-port DSP DB NTDW64 and 32-port DSP DB NTDW62 can be installed on the MGC. The DSP daughterboards support VoIP voice gateway resources on the MGC, reducing the need for separate Voice Gateway Media Cards.

Features and enhancements

The MGC provides the following features and enhancements:

- Increased processing power (10x over SSC)
- Increased memory capacity (128 MB vs 32 MB on SSC)
- Compact Flash for permanent storage
- Two expansion daughterboard sites
- Embedded Layer 2 switch supports enhanced dual homing
- Co-resident applications (Voice Gateway and Media Gateway Controller)
- Enhanced diagnostics
- Enhanced loadware patching
- Increased reliability

The MGC features allow for a reduction of CS 1000E hardware:

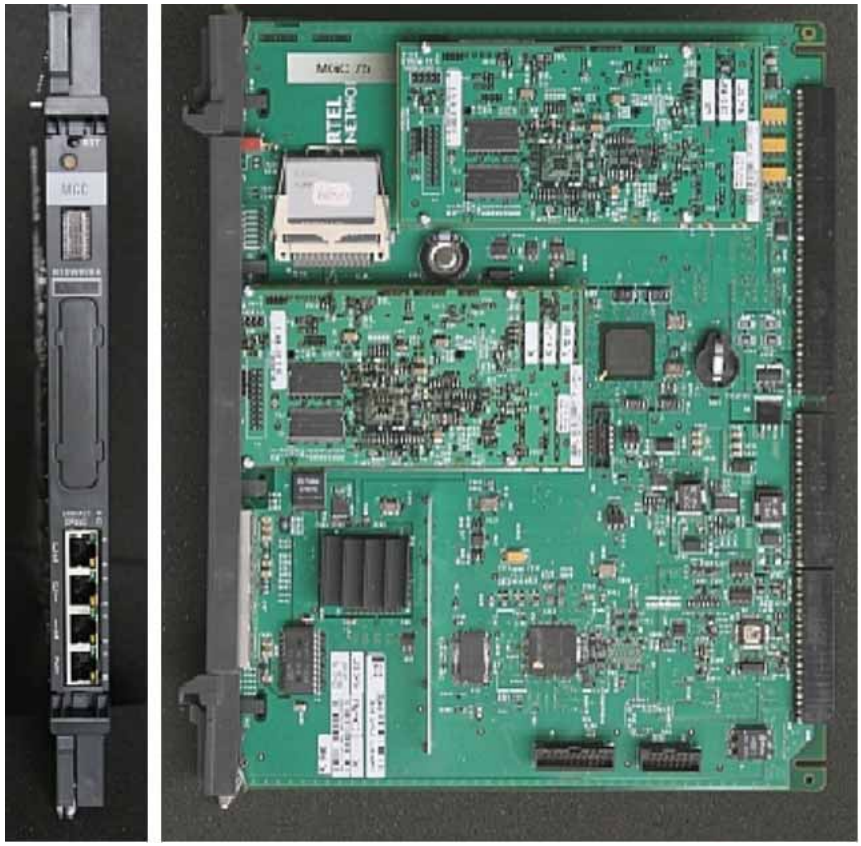
- Replaces the gateway control function in the MG 1000E.

- Reduces the need for Voice Gateway Media Cards with the use of MGC Digital Signal Processor daughterboards.
- Replaces MG 1000T peer gateways. MG 1000E with MGC supports PRI/PRI2/DTI/DTI2 trunks, BRI trunks, and clock controllers.
- Reduces the need for separate Terminal Servers with the MGC remote SDI feature.

Hardware description

Figure 2 "Media Gateway Controller card (NTDW60)" (page 28) shows the MGC faceplate and MGC circuit card (with both DSP daughterboards installed).

Figure 2
Media Gateway Controller card (NTDW60)



The MGC (without expansion daughterboards) includes the following components:

- Embedded DSP functionality.

The DSP resources are used to provide the following tone and conference functions:

— 60 tone generation channels grouped as two circuits (loops) of 30 units each.

— 16 DTR/XTD units. These resources can alternatively be configured as eight DTR/XTD units and four MFC/MFE/MFK5/MFK6/MFR units.

— 60 conference units grouped as two circuits (loops) of 30 units each.

- 128 MB of SDRAM (non-upgradeable).
- 128 MB Internal Compact Flash card mounted on the CPU card.
- Six 100 BaseT Ethernet ports for connection to external networking equipment (four ports on the faceplate and two ports on the backplane).
- A four-character LED display on the faceplate for displaying operational and diagnostic information.
- Two PCI Telephony Mezzanine card form factor sites for system expansion (daughterboard connections)
- Real Time Clock (RTC) with a capacitor hold-up for card reset or reseat, no battery backup
- Three Serial Data Interface (SDI) ports

Conference capacity

The MGC has a maximum of two conference loops, with 30 conference circuits for each conference loop, for a total of 60 conference circuits for each MGC-based MG 1000E. The maximum number of parties on a MG 1000E with MGC is 30.

- The MGC card supports

  — One loop per TDS definition (30 units per loop).

  — One loop per Conference definition (30 units per loop).

  — Can define up to two Conference loops and two TDS loops.

ATTENTION

If a CS 1000E system is equipped with a mix of SSC and MGC cards, and the MG 1000E with SSC has a conference loop configured, the maximum number of parties for any conference on the system is six.

If a SSC single-port IP daughterboard is used, define no more than three conference loops for that MG 1000E. With a single-port daughterboard, there is no way to determine if a fourth conference loop exists, so a fourth conference loop causes failures for accessing conference circuits.

Media security feature

The MGC DSP daughterboard security feature provides an infrastructure to allow endpoints capable of SRTP/SRTCP to engage in secure media exchanges. The media security feature can be configured by the administrator or, optionally, by the end user. This feature provides for the exchange of cryptographic material needed by the SRTP-capable endpoints to secure media streams originating from those endpoints.

For more information

Fore more information about the Media Gateway Controller, see *Circuit Card Reference (NN43001-311)*, *Communication Server 1000E Installation and Commissioning (NN43041-310)* and *Communication Server 1000E Upgrades (NN43041-458)*.

For more information about Media Security or SRTP, see *Security Management Fundamentals (NN43001-604)*.

DSP Daughterboard

Introduction

Two new DSP Daughterboards are introduced in Communication Server (CS) 1000 Release 5.0. These daughterboards are available in two different sizes:

- NTDW64AA 96-port DSP Daughterboard
- NTDW62AA 32-port DSP Daughterboard

These daughterboards are installed on the Media Gateway Controller (MGC), providing DSP resources to facilitate communication between IP and TDM devices. This eliminates the need for Voice Gateway Media Cards within the CS 1000E Media Gateway (MG 1000E) Chassis and/or Cabinet.

Configuration and maintenance

The DSP Daughterboard requires overlay configuration and overlay maintenance for the DSP TNs, as well as additional configuration for codecs. Maintenance and diagnostic commands are also available for use, similar to those used on the Voice Gateway Media Card. The DSP Daughterboards include the Voice Gateway application of the current Voice Gateway Media Card solution, but do not include the Terminal Proxy Server (TPS) application, which allows IP Phones to register with the Voice Gateway Media Card or Signaling Server.

For more information

For more information, refer to the following:

- *Communication Server 1000E, Installation and Commisioning (NN43041-310)*
- *Communication Server 1000E Upgrades (NN43041-458)*

MC32S Media Card

The MC32S is a 32-channel Voice Gateway Media Card that provides 32 Digital Signal Processor (DSP) ports to facilitate connectivity between IP and TDM devices.

This media card replaces the existing 32-port Voice Gateway Media Card and enables Secure Real Time Protocol (SRTP) to encrypt the IP media path to and from all DSP channels on the MC32S. The MC32S also provides improved echo performance over the existing media card.

For more information about the MC32S, refer to *IP Line Fundamentals (NN43100-500)*.

Resiliency

Communication Server (CS) 1000 Release 5.0 creates a system that provides more resiliency and robustness through the following enhancements:

- Geographic Redundancy Enhancements
  - "Geography Redundancy Survivable Media Gateway" (page 37)
  - "Network Wide Redundancy Phase II" (page 39)
- "CPP Redundancy and Resiliency Phase II" (page 41)
- "Diagnostic and Fault Reporting Enhancements" (page 45)
- "SNMP Enhancements" (page 47)
- "VTRK Failover Upon Network Failure" (page 51)

Geography Redundancy: Survivable Media Gateway

Description

The Geographic Redundancy: Survivable Media Gateway increases the reliability of CS 1000E systems by allowing up to 50 geographically remote Secondary Call Servers to be registered to a Primary Call Server. Each Secondary Call Server can be configured as Alternate Call Server 1 or Alternate Call Server 2.

Two levels of redundancy are provided:

- Primary Call Server failure: Local and remote resources register with the Secondary Call Server configured as Alternate Call Server 1.
- WAN failure: Local resources register with the secondary Call Server configured as Alternate Call Server 2.

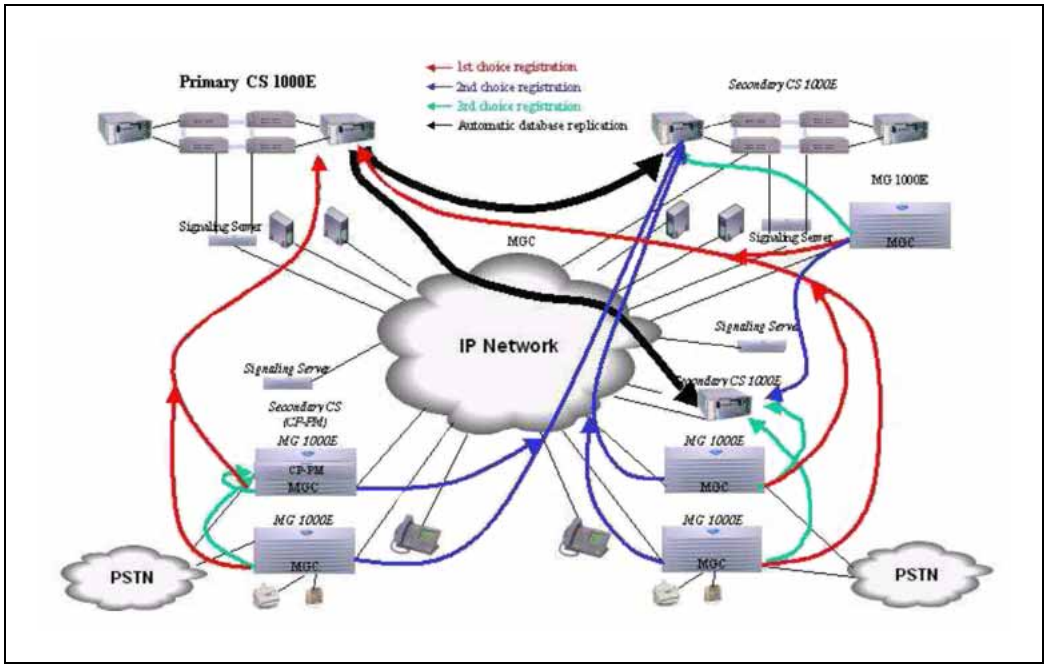
Redundancy is provided for both IP and TDM resources by allowing triple IP registration. Devices register to the Primary Call Server as first choice, Alternate Call Server 1 as second choice, and Alternate Call Server 2 as third choice. New commands are introduced to allow forced manual switching of Media Gateway 1000Es to a specified secondary Call Server.

The database is administered on the Primary Call Server and replicated to the Secondary Call Servers manually or by automatic scheduling. In LD 117, Geographic Redundancy Database Replication Control (GRDRC) associated commands now support a new backup mode, SCHD, which allows database replication to be automatically scheduled. Geographic Redundancy State Control (GRSC) commands now support up to 512 blocks, and there is a new threshold for the maximum number of Media Gateways that can be registered on a Secondary Call Server without causing the system to become active.

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

Figure 3 "Geographic Redundancy Survivable Media Gateway configuration" (page 38) shows a Survivable Media Gateway configuration:

Figure 3
Geographic Redundancy: Survivable Media Gateway configuration



Configuration of a Survivable Media Gateway system is performed using CLI or Element Manager.

For more details, refer to *System Redundancy Fundamentals (NN43001-507)*.

Network Wide Redundancy Phase II

Feature Description

This feature is an enhancement to the existing Branch Office User ID (BUID) Branch. The addition of a Temporary IP User license creates a new Network Wide Redundancy Network User ID (NUID) Branch that allows remote IP Phones to normally register with a central switch, the Network Home, which can be a Communication Server (CS)1000. In the normal mode of operation, these IP Phones are under the control of the Network Home and receive telephony services from it.

If the Network Home cannot be reached, the remote IP Phones register with a local CS 1000 in local mode to receive telephony services. This feature has no package dependency and is available to all systems equipped with the required License Limit.

Temporary IP User license

This enhancement limits the number of IP Phone Terminal Numbers (TN) which have 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 or Basic IP User licenses.

For more information on this feature, refer to *Features and Services Fundamentals - Book 5 of 6 (NN43001-106-B5)*.

CPP Redundancy and Resiliency Phase II

The CPP Redundancy and Resiliency Phase II feature enhances robustness and resiliency in the CPP system by addressing:

- Loss of calls due to ungraceful switchover
- Health monitoring
- Delays in switchover time
- System capability to recover from network outages

These enhancements are provided by the following elements of the feature:

- Survival of conference calls after system initialization

  With CS 1000 Release 5.0, conference calls on the CS 1000E are rebuilt after system initialization, including initialization due to an ungraceful switchover of cores. Calls are rebuilt using Network Control Memory. Also restored are established calls involved in add-on conference. The operation of meet-me conference calls is not affected.

- ACD Queue Call Recovery (ACDR) for CPP ungraceful switchover

  This enhancement restores transient calls in ACD queues during CPP ungraceful switchover. Data for transient calls is mirrored on the inactive core. After system initialization resulting from ungraceful switchover, this data is used to rebuild ACD queues. A maximum of 1000 calls can be restored. If, during system initialization, another system initialization is invoked (INI within INI), ACDR continues to restore calls.

- INI/SYSLOAD commands in LD 135

  Prior to CS 1000 Release 5.0, system initialization could be invoked only from the PDT shell. With CS 1000 Release 5.0, six new commands are available in LD 135 to invoke system initialization on the active and inactive cores.

- Reduced system-invoked Ungraceful Switchover trigger time

Heartbeat software is designed to monitor the status of the other side in a redundant system and provide information to trigger an ungraceful switchover. If the heartbeat cannot be communicated between the two CPUs, the redundant CPU warm starts and becomes 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 in CS 1000 Release 5.0. The optimization of timing leads to a change in the INI policy. When the active core warm starts, the inactive core also reboots. Therefore, there is no swapping of cores.

- Reduced Graceful Switchover time

  The reduction of graceful switchover time depends mainly on the amount of data that the system must copy to the inactive side prior to switchover. To optimize the amount of data being copied, Stop and Copy in CS 1000 Release 5.0 includes a checksum mechanism to ensure mirror imaging of data on both cores of a redundant system. The checksum mechanism :

  — 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

- Write-protect memory on inactive side

  Because the inactive side performs many background tasks and operations, it is susceptible to memory corruption in Protected Data and Protected Heap. In CS 1000 Release 5.0, a write-protect mechanism is activated after every update and protected memory synchronization. This protects data and heap memory from corruption. A write-protect violation is triggered if there are any unauthorized attempts to write to protected memory.

- Graceful Switchover failure and recovery

  Previously, a Stop and Copy failure during graceful switchover left duplicate IP addresses on the High Speed Pipe link, causing a failure in communication between active and inactive cores. To restore redundancy, the inactive core had to be manually restarted.

  With CS 1000 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.

- Fine tune health update to prevent premature Graceful Switchover

The active core must have the most recent health update/status of the remote Call Server before attempting a graceful switchover. Otherwise, a graceful switchover be initiated prematurely and subsequently fail. This feature prevents this scenario.

A health update is initiated from the inactive core before a graceful switchover. This ensures that the remote Call Server is ready.

Diagnostic and Fault Reporting Enhancements

The Diagnostic and Fault Reporting Enhancements for Communication Server (CS) 1000 Release 5.0 are designed to reduce costs by adding diagnostic and reporting tools that shorten Mean Time to Repair.

Diagnostic enhancements

The following diagnostic enhancements include improved utilities specific to Voice Gateway Media Card resources, more useful message trace tools, and better operational measurements:

- DSP Audit Routine:
  Error reporting for Voice Gateway channels is logged on the Call Server, eliminating the need to search all Voice Gateway Media Cards for the faulty Voice Gateway channel.
- LD 80 Trace Enhancement:
  Primary enhancements in LD 80 include:
  - new output in VoIP conference traces.
  - increased detail in virtual trunk call traces.
  - a new call trace for IP Phones.
- SIP Call Trace Enhancement:
  This feature both simplifies output and provides more detail by:
  - removing repetitive information.
  - adding several output fields to **`SipCallTrace`** Level 0 and Level 1 commands.
- Infinite Loop Code Conversion:
  Infinite loop codes are converted to have only one function call inside the loop. This eliminates the need to patch the loop. Instead, only the function called from inside the loop must be patched (if required), and it is no longer necessary to restart the task containing the infinite loop.

- DCH Trace Tool Enhancement:
  A new Call Server log file for DCH trace messages provides the flexibility to save messages for later retrieval. LD 96 includes six new commands for specifying the output location of DCH trace messages.
- SIP and H.323 Gateway Registration Trace Messages:
  This feature introduces two new CLI commands that trace Registration messages at the SIP gateway and at the H.323 gateway. The commands are available at both the OAM and the PDT shells. Output options include TTY, RPT, or log file, consistent with existing functionality.

Fault reporting enhancements

The following fault reporting enhancements include improved mechanisms for identifying abnormal conditions during installation, startup processes, or during tests or audits:

- Voice Gateway failure log on Call Server:
  New system alarms are generated for DSP channel problems, and in the case of a critical error, an SNMP trap is issued. Depending on whether the ELAN link is up or down, messages are sent to the Call Server and the Voice Gateway Media Card, or to the Voice Gateway Media Card only.
- Voice Gateway sanity testing:
  Sanity testing during reboot of a Voice Gateway Media Card prevents the Call Server from using faulty DSP channels. If the sanity test finds an error, the DSP channel is blocked from registration and a sanity test report, which includes a system alarm message, is generated.
- Audit of File Descriptor usage:
  Usage of File Descriptors (FDs) is monitored in a background audit routine that triggers a warning message or SNMP trap when the number of available FDs is below certain thresholds. Updated CLI and LD 135 commands facilitate manual monitoring of File Descriptor usage.
- Audit of Heap Memory usage:
  Usage of Heap Memory is monitored in the same background audit routine that monitors File Descriptors, and with the same LD 135 command. This feature also introduces a Patching Capacity Utilization Report.

SNMP Enhancements

Description

Support for the Simple Network Management Protocol (SNMP) is enhanced to simplify the provisioning and use of SNMP for fault management and system health monitoring of the CS 1000 and Meridian 1 systems.

Enhancements

The functional features introduced in this release include simplified configuration and synchronization of SNMP parameters, and changes to the trap generation mechanism of CS 1000 and Meridian 1 system devices.

System devices that support SNMP include:

- Call Servers
- Signaling Servers
- Voice Gateway Media Card
- Media Gateway Controller (MGC)
- Network Routing Server (NRS) on Linux
- Enterprise Common Manager (ECM)

The following sections describe the enhancements to SNMP for fault management and system health monitoring:

Single point of configuration

You can use a single point of configuration to configure the SNMP parameters on the Call Server. The configuration is synchronized to Signaling Servers, Voice Gateway Media Cards, and MGCs when an Equipment Data Dump (EDD) is performed.

Synchronization does not occur on Linux systems; therefore, SNMP configuration is done on each element manually.

Common Trap MIB

Previously, each CS 1000 device (such as the Call Server, Signaling Server, Voice Gateway Media Cards, and IP Trunk cards) used its own trap MIB to define the format for its own specific traps.

In CS 1000 Release 5.0, a Common Trap MIB (COMMON-TRAP-MIB.mib) is defined with new trap object identifiers (OID) that provide a common format for all elements.

Configurable Trap community string

The Trap community string (SYSMGMT_TRAP_COMM) is configurable in CS 1000 Release 5.0. Use two new commands, CHG SYSTEM_TRAP_COMM and PRT SYSTEM_COMM, to change and print the Trap community string. Configure the Trap community string in LD 117 by using a Command Line Interface (CLI) or Element Manager.

Network routing table entries

The Call Server has a single ELAN network interface, while the Signaling Server, Voice Gateway Media Card, and MGC have both ELAN and TLAN network interface connections. When SNMP is used to send traps from a device with both ELAN and TLAN network interfaces, it is necessary to specify the network interface (for example, ELAN) and gateway to be used. Use the ELAN network interface to send out SNMP traps on all of the devices.

In previous releases, the network routing table entries were entered manually for the Signaling Server and Voice Gateway Media Card by using Element Manager. In CS 1000 Release 5.0, the associated host route entries for new trap destinations are added automatically to the network routing table for the Signaling Server, Voice Gateway Media Cards, and MGCs.

MIB II System group

In CS 1000 Release 5.0, the *sysDescr* format is changed. The *sysDescr* format is a name-value pair of applicable attributes with the value enclosed in quotes for easier parsing.

SNMP support for Linux systems

SNMP is implemented on Linux systems by using an SNMP agent, and SNMP parameters are configured by using the SNMP configuration page. The Net-SNMP Agent includes an implementation of MIB-II objects, and SNMP traps are in the Common Trap format.

Linux applications, which can run on various hardware platforms, include Enterprise Common Manager (ECM) and Network Routing Service (NRS).

Synchronization does not occur on Linux systems; each element is configured individually.

SNMP support for new hardware

For new hardware, support exists for SNMP queries and SNMP traps. The new hardware includes the Media Gateway Card (MGC), the Media Card 32S (MC32S), and Common Processor Pentium Mobile (CP PM) Card.

In addition, support exists for commercial off-the-shelf (COTS) system servers.

Refer to *Communication Server 1000 Fault Management — SMNP (NN43001-719)* for additional information on these features.

VTRK Failover Upon Network Failure

Overview

The VTRK Failover Upon Network Failure feature, which enables Virtual Trunk (VTRK) calls to survive a network failure.

Upon network failure, the Leader Signaling Server is isolated from the rest of the network which, caused it to unregister its VTRKs from the Call Server. In the meantime, the Follower Signaling Server did not receive the Leader *I'm Master* broadcast message so an election is called and the Follower Signaling Server becomes the master. As a result, the VTRK application attempts to register with the Call Server. The Call Server grants the request since the Leader Signaling Server already sent a server offline message. VTRK calls are now made through the Follower Signaling Server.

Once the network connection is reestablished, an election is called again. The Follower Signaling Server relinquishes mastership and unregisters its VTRKs from the Call Server. The Leader Signaling Server is able to reregister VTRKs. VTRK calls are now made through the Leader Signaling Server again.

Description

The VTRK Failover Upon Network Failure feature implements the VTRK Network Health Monitor to monitor the health of the network, which is configured using Element Manager.

The VTRK Network Health Monitor task starts when the Signaling Server boots. The VTRK Network Health Monitor task receives a request from the Signaling Server applications to monitor the connectivity status of a given IP address. The Virtual Trunk uses this monitor task to send ping messages to the list of preconfigured IP addresses.

The monitored IP addresses are read from the config.ini file. The following example shows a sample of the new section in the config.ini file with VTRK Network Health Monitor task configured using Element Manager.

Config.ini file with VTRK Network Health Monitor task enabled

```
[VTRK NETMON]
```

```
ENABLE = 1
IP = 192.168.2.1
IP = 192.168.2.10
```

If VTRKNETMON section is not present, or if there is no valid IP address, then the TLAN Gateway is monitored by default.

The following parameters apply to the config.ini file:

- ENABLE—specifies if the VTRK Network Health Monitor monitors IP addresses or not. If there is no value present, the IP addresses are monitored by default.
  - — ENABLE = 1 (VTRK Network Health Monitor monitors IP addresses)
  - — ENABLE = 0 (VTRK Network Health Monitor does not monitor IP addresses)
- IP — specifies all IP addresses to be monitored by the VTRK Network Health Monitor. Invalid IP address formats are ignored.

If at least one IP address in the monitored list is reachable and the Signaling Server is Leader, the Virtual Trunks remain registered with the Call Server. If all monitored IP addresses are unreachable, the Leader Signaling Server unregisters its Virtual Trunks to enable the Follower Signaling Server to register with the Call Server and take over the Virtual Trunk operation.

The VTRK Network Health Monitor sends ICMP PING requests every ten seconds to each monitored IP address. If no response is received within five seconds, five more PING retries are sent, one second apart. If there is still no response, the IP address is considered unreachable. The detection time for each IP address is between 10 and 20 seconds.

When all monitored IP addresses are determined unreachable and the Signaling Server is Leader, the Virtual Trunks are unregistered from the Call Server. In the meantime, this isolated Signaling Server continues to monitor the network status by pinging all monitored IP addresses every ten seconds. When the network recovers, the Signaling Server reregisters the Virtual Trunks if it is the node Master. If only a subset of all monitored IP addresses are unreachable, the Signaling Server maintains its Virtual Trunk registration, and all IP addresses, whether they are reachable or not, are pinged every ten seconds.

As soon as one ping response is received, the corresponding IP addresses is determined reachable. If the isolated Signaling Server is the Leader, it attempts to register its Virtual Trunks with the Call Server. If this Signaling Server is the Follower, it ignores this event and continues to monitor the list of IP addresses by sending a PING request every ten seconds.

Although the monitored IP addresses are pinged separately, they are read from the config.ini file and are monitored at the same time when the Signaling Server boots. Thus, the time to detect a network failure is between 10 and 20 seconds

Administration and maintenance

The oam CLI prompt is added to the **oam > shell**.

Table 1
New CLI prompt

Prompt	Response	Description
oam	vtrkNetMonShow	Print the current list of monitored IP addresses and their status.

Element Manager configuration

Use Element Manager to configure the following new functionalities:

- VTRK Network Health Monitor configuration for an IP Telephony node
- VTRK Network Health Monitor CLI commands support for an IP Telephony node

VTRK Network Health Monitor configuration for an IP Telephony node

Login to Element Manager. Navigate to **IP Network > Nodes: Servers, Media Cards** to open the Node Configuration window to begin configuration.

Adding an IP address to VTRK Network Health Monitor

Step	Action
1	Enter a node number in the New Node field or expand a configured node.
2	Expand the VTRK Network Monitor configuration window.
3	Click **Add**.
4	Expand the Virtual Trunk Network Health Monitor configuration window. The Monitor check box is selected by default.
5	Click **Add** beside Monitored IP address to add a new IP address field. Once the maximum of 8 IP address fields is reached, the Add button is disabled.

6 Enter a valid IP address.

7 Click **Save and Transfer**.

—End—

Editing a monitored IP address in VTRK Network Health Monitor

Step	Action
1	In the Node Configuration window, click the **Edit** button of a node.
2	Expand the VTRK Network Monitor configuration window.
3	Edit the configured monitored IP address.
4	Select or deselect the Monitor check box. If the Monitor check box is deselected, the **Add** button beside Monitored IP address and the **Add** button beside each monitored IP address rows is disabled.
5	Click **Save and Transfer**.

—End—

Viewing new CLI commands in Element Manager

Step	Action
1	Login to Element Manager. Navigate to **IP Network > Maintenance and Reports**.
2	Expand a configured node.
3	Click **GEN CMD** against a Signaling Server element.
4	Select **Vtrk** from the Group dropdown list.
5	Select **vtrkNetMonShow** from the Command drop down list.
6	Click **Run**.

—End—

Deleting a monitored IP address in VTRK Network Health Monitor

Step	Action
1	In the Node Configuration window, expand the Node.
2	Expand the VTRK Network Monitor configuration window.
3	Click the **Remove** button beside a configured monitored IP address to delete it.
4	Click **Save and Transfer**.

—End—

Table 2
VTRK Network Monitor button description in Element Manager

Action	Response	Comment
Monitor	Check box	Selected by default. If selected, ENABLE = 1 If deselected, ENABLE = 0.
IP address	128 bit IPv4 address in the format: xxx.xxx.xxx.xxx	Each row caption is suffixed with the number of rows. Up to 8 IP addresses are configured. Config.ini stores these values in the following format: [VTRK NETMON] ENABLE = 1 IP = 47.11.221.22 IP = 47.11.221.23
Click the Check box	If the check box is selected, the Add and Remove buttons are enabled. If the check box is deselected, the Add and Remove buttons are disabled.	When the Monitored check box is deseleted, all configured IP addresses, and the Add and Remove buttons are disabled.
Click the Add button	A new row appears to enter a Monitored IP address.	The Add button is enabled if the number if IP address rows are less than 8. The Add button is disabled after 8 rows

		of IP addresses are displayed and when the Monitor check box is deselected.
Click the Remove button	The Monitored IP address row is deleted and the next row caption changes to reflect the current row number.	Click the Remove button beside the Monitored IP address to delete the IP address. If the Monitor check box is deselected, the Remove button is disabled.

VTRK Network Health Monitor Configuration CLI commands

Login to Element Manager. **Navigate to IP Network > Maintenance and Reports**.

Running the vtrkNetMonShow command

Step	Action
1	Expand a configured node.
2	Click the **GEN CMD** button against a Signaling Server element.
3	Select **vtrk** from the Group drop down list.
4	Select **vtrkNetMonShow**.
5	Click **Run**.

—End—

New SNMP alarms

The following new SNMP alarms are created on the Signaling Server:

- ITG4121

  Message: “Monitored IP: <%s>: Fail Retry”
  Description: this is created when a ping was sent to an IP address and no response was received within five seconds. Five more pings are sent and didn’t receive response in Five seconds. Five more pings are to be sent one second apart before it is determined that the IP address is unreachable. This alarm is created by tNetMon task.
  Severity: Warning

- ITG5121

  Message: “Monitored IP <%s>: OK”
  Description: this is created when a ping response was received for a previously unreachable IP address. This alarm is reported by tNetMon Task

Severity: Clear

- ITG1121

  Message: “Monitored IP <%s>: Unreachable”
  Description: this is created when five ping retries failed; that is, no response was received. This alarm is reported by tNetMon Task
  Severity: Critical

- ITG1122

  Message: “Virtual Trunk Network is: Down”
  Description: this alarm is created by VTRK task when all the monitored IP addresses are determined to be unreachable and this Signalling Server is current node master.**Severity:** Critical

- ITG5122

  Message: “Virtual Trunk Network is: OK”
  Description: this alarm is created by VTRK task when the first "IP reachable" event occurs to clear the “isolation” alarm.
  Severity: Clear

Open Interoperability

Communication Server (CS) 1000 Release 5.0 further integrates SIP into all aspects of the system and provides systems with more open interoperability through the following support and enhancements:

- "SIP NRS on Linux" (page 61)
- "Dual Tone Multi-frequency (DTMF) Handling using RFC2833" (page 63)
- "Network Time Protocol" (page 67)
- "Nortel Converged Office" (page 87)

CS 1000 Release 5.0 enhances the desktop clients to provide SIP functionality which enables these devices to operate third-party systems.

Network Routing Service on Linux

Network Routing Service

The Network Routing Service (NRS) provides routing to SIP and H.323 compliant devices. The network protocol component of the NRS is comprised of:

- SIP routing
- H.323 Gatekeeper
- Network Connection Service

NRS for CS 1000 Release 5.0 software is offered in two versions: one that includes a SIP Redirect Server and one that includes a SIP Proxy.

The NRS with a SIP Redirect Server is either hosted co-resident with Signaling Server applications, or in a stand-alone mode on a dedicated Common Processor Pentium Mobile (CP PM) server running the VxWorks™ real-time operating system. There are no changes to the SIP Redirect Server NRS in CS 1000 Release 5.0.

The NRS SIP Proxy is hosted in a stand-alone mode on a dedicated commercial off the shelf server running the Linux™ real-time operating system. The SIP Proxy NRS is referred to as the Linux-based NRS.

SIP Proxy

Communication Server (CS) 1000 Release 5.0 adds a transaction stateful SIP Proxy to the IP Peer Network.

A SIP Proxy acts as both a server and a client. A SIP Proxy receives requests, determines where to send the requests, and acting as a client on behalf of SIP endpoints, passes requests to another server.

A SIP Proxy makes the following features and functionality, which are provided by CS 1000 Release 5.0, possible:

1. Transport Layer Security (TLS).

TLS provides the NRS with private, secure signaling, message authentication, confidentiality, and integrity through end-to-end encryption of media exchanged between two SIP endpoints.

2. Mixed transport layer protocol.

   A mixed transport layer protocol enables gateways using TCP, TLS over TCP, or UDP to interoperate.

3. Network features.

   By default the SIP Proxy and Redirect Server functions as a SIP Proxy. However, an endpoint can request transaction by transaction that the SIP Proxy act as a SIP Redirect Server.

   A SIP Redirect Server receives requests, but does not pass the requests to another server. Instead, a SIP Redirect Server sends a response back to the SIP endpoint, indicating the IP address of the called user.

4. Post-routing SIP URI modification.

5. Transaction forking.

NRS database

The Linux-based NRS provides real-time synchronization of the databases on the Primary and Secondary Network Routing Servers.

NRS Manager

NRS Manager is a web-based management application used to configure, provision, and maintain the NRS. Key usability improvements introduced in the Linux-based NRS Manager are:

- Enhanced searching and sorting capabilities including wild cards and selectable scope of the search
- Capability to copy and move routing entries
- Simplified configuration for geographic redundancy
- Routing tests are fully integrated with endpoint and routing entry configuration
- SIP phone context mapping tools are fully integrated with endpoint and routing entry configuration
- Security infrastructure provided by the Enterprise Common Manager framework

For more information about the features discussed in this chapter, see *Network Routing Service Installation and Commissioning (NN43001-564)*

Dual Tone Multi-frequency (DTMF) Handling using RFC2833

Dual Tone Multi-frequency (DTMF) Handling using RFC2833 is a mechanism for transporting DTMF across a network. RFC2833 allows DTMF digits to be transmitted as a Real Time Protocol (RTP) payload for DTMF signaling. DTMF digit handling using RFC2833 allows Communication Server (CS) 1000 products to inter-operate with other SIP products that do not support DTMF signaling in-band.

This feature applies to all models of CS 1000 systems that utilize SIP trunking and covers the mandatory portion of RFC2833 which are the DTMF signals (0-15).

CS 1000 systems can send and receive digits in the following ways:

- tone as audio
- out-of-band signaling
- RFC2833

In CS 1000 Release 5.0, RFC2833 provides digit handling for DTMF signaling. With RFC2833, CS 1000 systems can inter-operate with SIP-based devices that do not support out-of-band DTMF digit signaling.

RFC2833 can be used for Session Initiation Protocol (SIP) calls only. H.323 and local calls are not supported.

With RFC2833, a key press on a UNIStim IP Phone is translated to an event packet that flows with the Voice over Internet Protocol (VoIP) stream to the far end. The event packet is an RFC2833 packet that contains the DTMF key that was pressed.

Table 3
Updated and new commands to support RFC2833

Command	Description
STAT RFC2833 <TN>	Prints the RFC2833 for the given TN. Updated LD 117. The stat RFC2833 command prints the RFC2833 capabilities for the TN, where the TN is either an IP Phone TN or Voice Gateway TN.
trac	trac <TN> prints the RFC2833 information for the given TN. The trac command is in LD 80.
vgwShow	Shows if RFC2833 is used for the current call.
sipNpmSessionShow	Shows RFC2833 information on a per-call basis.
sipNpmSIPTraceShow	Shows SDP messages: rtpmap and fmtp lines.
isetShow	Prints RFC2833 information.
ENL/DSL RFC2833PRT	The ENL/DIS command turns on/off the printing of the info message on a TTY port when Voice Gateway TN is allocated for a SIP call. This message includes the counter (counts how many times the RFC2833 uncapable VGW TN is selected for the SIP call). Element Manager is changed to include this command.

Set payload type

RFC2833 Rx capabilities for Voice Gateway TNs and IP Phones are stored in the RLM table. If RFC2833 is supported for a given Voice Gateway TN or IP Phone, the SIP Gateway negotiates RFC2833 capabilities with the far end using Session Description Protocol (SDP), during the SIP call set up. The negotiation is on a per-call basis.

CS 1000 Release 5.0 implementation of RFC2833 supports Dynamic Payload Type. When offering the use of RFC2833, the SIP Gateway includes the default value of 96 for the payload type and default clock rate of 8000 (8 kHz). The “fmtp“ line contains only DTMF events (0-15).

Below is an example of an SDP offer:

```
SDP v=0 c=IP IP4 a.b.c.d m=audio <udpport> RTP/AVP 18 0 3 19
96 a=ptime:20 a=rtpmap:96 telephone-event/8000 a=fmtp:96 0-15
<udpport>
```

Setting the payload type

Step	Action
1	On the Call Server at the PDT prompt, set the default payload type to another value.

For example, if the current value is 96 and you want to change it to 102, type:

```
pdt> setRFC2833PT 102
```

2 To confirm that RFC2833 Rx PT is 102, type:

```
pdt> setRFC2833PT 102
```

—End—

It is necessary to enter the RFC2833PT command in the start up file.

Entering the RFP2833PT command in the start up file

Step	Action
1	Locate the start up file named **/p/startup**
2	Type the following command the file at the end (where nnn = the payload type value) **setRFC2833PT 102 <enter>**
3	INI (or coldstart) the Call Server.
4	During INI, press **CTRL+B** when prompted, then press **c** to change the parameters. Press **<enter>** until the start up scripts prompt displays.
5	Type **/p/startup <enter>**. Continue to press **<enter>** until the end.
6	Press @ **<enter>** to continue to reboot.

—End—

Network Time Protocol

Feature description

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

Time distribution across the network

The NTP server obtains true time from the dedicated source, then sends that time to the Call Server, either directly over routers, or by proxy through the Signaling Server (depending on user configuration). The Call Server then distributes the time to the rest of the network.

NTP Server

CS 1000 Network Time Protocol can accommodate one or two NTP servers on the system: one primary server for regular operation (mandatory), and an optional secondary server for backup in case of primary failure. To enable the NTP feature, you must input the IP address of your primary and (if applicable) secondary servers.

Mode of communication

CS 1000 Network Time Protocol supports two modes of communication:

- Call Server to NTP server over ELAN subnet.
- Call Server to NTP server through the Signaling Server.

Call Server to NTP over ELAN subnet

With this mode of communication, the Call Server sends time requests to the NTP server over the ELAN subnet. The firewall provides ELAN subnet security. After the Call Server receives the time from the NTP server, it then distributes that time to nodal components on the network.

Call Server to NTP through the Signaling Server

With this mode of communication, the Signaling Server acts as the proxy for time request transfers between the Call Server and the NTP server. This mode of communication uses a TLAN subnet connection between the Call Server and NTP server, thus enhancing security.

NTP threshold levels

If the time difference (delta) between the Call Server and the NTP server passes certain threshold limits, the system generates alarm messages according to the severity level: Minimum, Warning, or Critical. Use LD 117 to increase or decrease the limits for these thresholds.

During manual synchronization, if the delta passes any of the threshold levels, the system generates an error message and asks if you want to update the time. Click **Yes** to accept the time change, or **No** to revert to the system time before the latest synchronization. During background synchronization, if the delta passes any of the threshold levels, the system generates the appropriate error message, but updates the time without asking for user confirmation.

Secure mode of operation

CS 1000 Network Time Protocol can operate in secure or insecure mode. In secure mode, the protocol uses Message Digest Algorithm 5 (MD5) signatures to authenticate the exchange of timestamps. To run NTP in secure mode, configure the following security parameters:

- Key ID: a number used to generate the message-authentication code
- Private Key: a secret key shared by the CS 1000 system and the NTP server, used to encrypt the MD5 value

Time zone

You must configure the offset between your local time zone and Coordinated Universal Time (UTC). The UTC offset corrects the timestamp according to the offset value entered by the user in LD 117 or Element Manager.

Daylight-Saving Time

If Daylight-saving time applies to your local time zone, then you must implement the Daylight-saving adjustment in LD 2 or from Element Manager.

Mode of synchronization

With NTP enabled, you can then synchronize the time across the CS 1000 network to the NTP server. NTP supports two modes of synchronization:.

- manual
- background

Manual mode of synchronization

Manual mode allows for a single, system-wide update of local system clocks to NTP server time. You can perform the manual update from LD 117 or Element Manager.

Background mode of synchronization

In background mode, the Call Server queries the NTP server at regular time intervals, as specified in LD 117 or Element Manager. When using background mode, you must also specify an offset value (in minutes) by which NTP avoids interfering with other scheduled background routines.

NTP status

With CS 1000 Network Time Protocol, use the STAT NTP command in LD 117 to check the current status of NTP. Status information displays in four categories—current NTP configuration, last NTP configuration, last synchronization error, and counters—and includes the following fields:

- NTP enabled or disabled (if disabled, the report includes no further information).
- IP addresses of the primary and secondary NTP servers
- local time zone offset from UTC
- time difference (delta) between system time and NTP server
- current threshold level: Minimal, Warning, Maximum
- secure mode of operation set to secure or insecure
- packets sent
- packets received

NTP status information also appears on the Date and Time page in Element Manager, under the Network Time Protocol field.

Print NTP parameters

With CS 1000 Network Time Protocol, use the PRT NTP command in LD 117 to display the current configuration of NTP. Displayed parameters include:

- IP addresses of primary and secondary NTP servers
- values for the three threshold levels: Minimum, Warning, and Maximum
- security mode: secure or insecure
- Key ID (if NTP is running in secure mode)
- time interval
- local time zone offset from UTC

- synchronization mode: manual or background

Feature interactions

Network Time Synchronization

CS 1000 Network Time Protocol and Network Time Synchronization (NTS) are mutually exclusive features. If you enable NTP, you cannot then make the NTS slave active. Any attempt to do so results in an error message indicating that you should disable NTP. Similarly, if you make the NTS slave active, you cannot then enable NTP. If you attempt to enable NTP, the Call Server sends an error message indicating that you should disable the NTS feature.

Geographic Redundancy

The Geographic Redundancy feature replicates databases from one Call Server to a secondary Call Server in a physically-distanced location. However, because many NTP parameters depend on location—UTC offset, for example—the NTP database does *not* replicate to the secondary Call Server. Therefore, the NTP configuration does not survive a geographic redundancy switchover.

Call Detail Recording

Call Detail Recording (CDR) identifies the calling and called parties and notes the time and duration of the call. If an NTP synchronization takes place between the start time and end time of the call, the duration for all segments of the call can become inconsistent, with some timestamps generated before the synchronization took place, and some generated afterwards.

Traffic Analysis

In Traffic Analysis, calculating the time it takes the system to transfer collected data depends on the current time of the system. If NTP synchronization changes system time during a period of heavy traffic, this can affect the time calculation. If traffic analysis has already been done for that hour, the system does not try to update the time again during that particular hour.

Call accounting/call tracking

Accurate call accounting/call tracking depends on accurate call start and end times. If the NTP time update takes place between the start and end of a call, disruption of accurate billing can occur.

Manual time updates using LD 02

With NTP enabled, you cannot manually update the system clock from LD 02. If you attempt a manual time update from LD 02, the Call Server generates an alarm indicating that NTP is running and that, to change the time manually, NTP must be disabled in Element Manager or LD 117.

Attendant Console Time and Date key

With NTP enabled, the system protects accuracy and reliability of network time by restricting manual time changes using the Time and Date key on Attendant consoles. If you attempt a time change using the Time and Date key, the Call Server generates an alarm indicating that NTP is running and that, to change the time manually, NTP must be disabled in Element Manager or LD 117.

Feature implementation using LD 117

Use these procedures to implement the CS 1000 Network Time Protocol in LD 117.

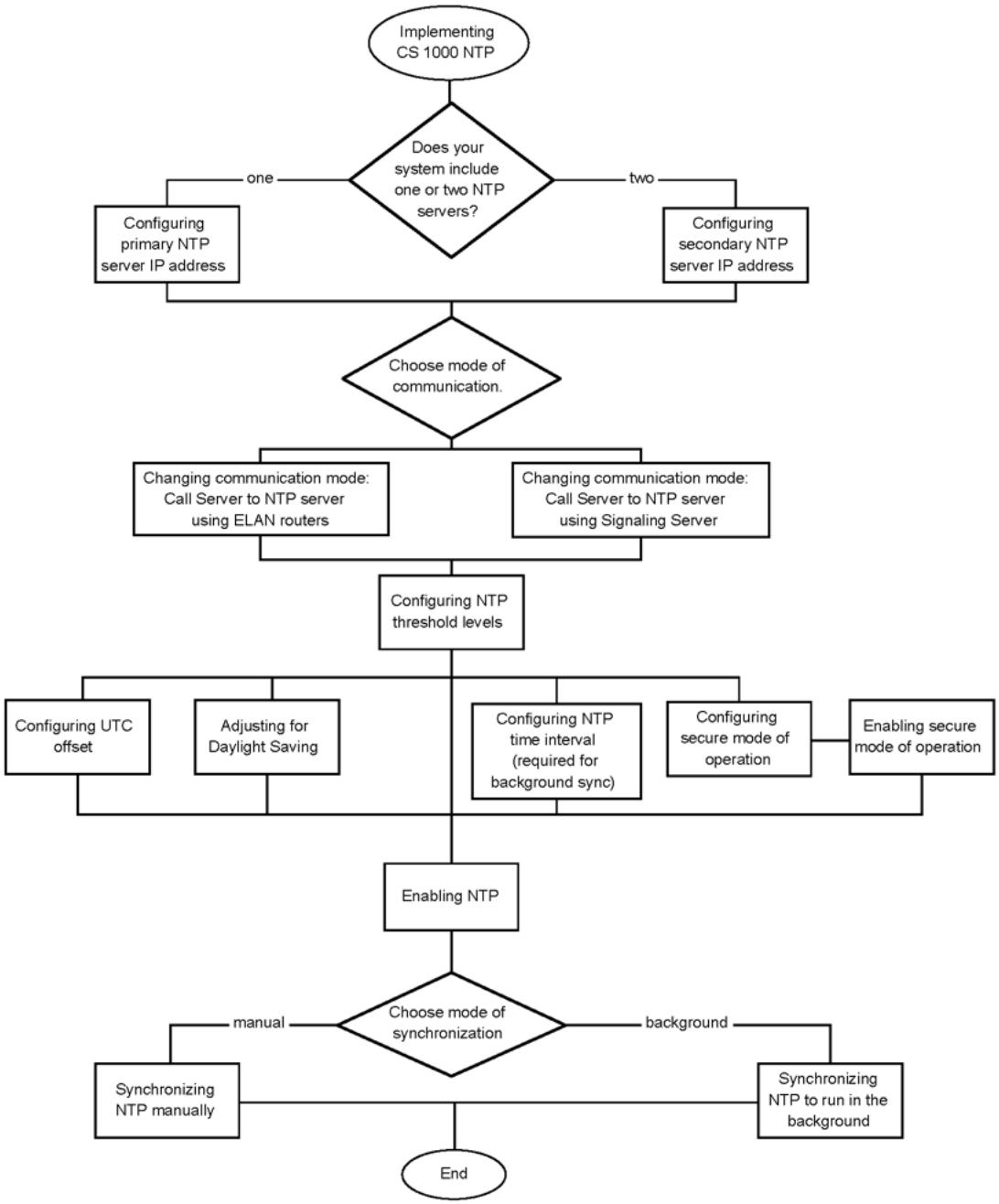
Prerequisites for implementing NTP using LD 117

- You must have at least one NTP server available to the system.
- For full access to NTP maintenance commands in LD 117, login with Admin2 (PWD2) status. If you login without PWD2, some commands do not run.
- Before you start, obtain the IP addresses for your primary and (if included on the system) secondary NTP servers.
- To configure any NTP parameter from LD 117, NTP must be disabled. See "Disabling NTP" (page 79).
- Configure a valid IP address for your NTP server before configuring any other NTP parameter. Failure to do so results in an error message.

Procedures for implementing NTP using LD 117

This task flow shows the sequence of procedures to implement the CS 1000 Network Time Protocol. To link to any procedure, see "Procedures for implementing NTP using LD 117" (page 73)

Figure 4
Implementing NTP procedures using LD 117



Procedures for implementing NTP using LD 117

- "Configuring primary NTP server address" (page 73)
- "Changing communication mode: Call Server to NTP server over ELAN subnet" (page 74)
- "Changing communication mode: Call Server to NTP server using Signaling Server" (page 74)
- "Configuring NTP threshold levels" (page 75)
- "Configuring NTP Time interval" (page 75)
- "Configuring secure mode of operation" (page 76)
- "Enabling secure mode of operation" (page 77)
- "Disabling secure mode of operation" (page 77)
- "Configuring UTC offset for local time zone" (page 78)
- "Adjusting for Daylight Saving Time" (page 78)
- "Enabling NTP" (page 78)
- "Disabling NTP" (page 79)
- "Synchronizing NTP to run in the background" (page 79)
- "Synchronizing NTP manually" (page 80)
- "Checking NTP status" (page 81)
- "Printing NTP parameters" (page 81)

Configuring primary NTP server address

Use this procedure to enter the IP address of the primary NTP server.

Procedure steps

Step	Action
1	Login to LD 117.
2	Input the IP address of the primary NTP server `CHG NTP <primary NTP server IP address>`

—End—

Configuring secondary NTP server IP address (optional)

Use this procedure to enter the IP address of the secondary NTP server.

Procedure steps

Step	Action
1	Login to LD 117.
2	Enter the IP address of both the primary and secondary NTP servers. `CHG NTP <primary NTP server IP address> <secondary NTP server IP address>`

ATTENTION
When configuring the secondary IP address, enter both primary and secondary addresses together at the prompt.

—End—

Changing communication mode: Call Server to NTP server over ELAN subnet

Use this procedure to change the mode of communication to: Call Server to NTP server over ELAN subnet.

Procedure steps

Step	Action
1	Login to LD 117.
2	Use the following command to change the mode of communication to: Call Server to NTP using router. `CHG NTP MODE CS`

—End—

Changing communication mode: Call Server to NTP server using Signaling Server

Use this procedure to change the mode of communication to: Call Server to NTP server using Signaling Server.

Procedure steps

Step	Action
1	Login to LD 117.

2 Use the following command to change the mode of communication to: Call Server to NTP using Signaling Server.

```
CHG NTP MODE SS
```

—End—

Configuring NTP threshold levels

Use this procedure to configure the three NTP threshold levels: Minimum, Warning, and Maximum.

Procedure steps

Step	Action
1	Login to LD 117.
2	Enter desired values for the three threshold levels. Do not use leading zeroes. For example, to enter a value of seven minutes, type `7` not 00:07. `CHG NTP THRESH <minimum> <warning> <maximum>`

ATTENTION

Enter values for all three threshold levels whenever you use the CHG NTP THRESH <minimum> <warning> <maximum> command.

—End—

Configuring NTP Time interval

Use this procedure to configure both the time interval for background synchronization and the offset from other background routines.

ATTENTION

Configure the NTP time interval before you attempt to enable background synchronization.

Procedure steps

Step	Action
1	Login to LD 117.
2	Enter the time interval and offset value for background synchronization. Do not use leading zeroes. For example, to enter a value of six minutes type `6` not `00:06`.

```
CHG NTP TIMEINT <time interval in minutes> <offset in
minutes>
```

—End—

Procedure job aid

Field	Description
<time interval in minutes> **<offset in minutes>**	To change the time interval for background synchronization, enter one of the following standard values (in minutes): 1, 2, 6, 12, (24), and 30. Default time interval is 24 minutes between background synchronizations. To change the offset value from which synchronization avoids other background routines, enter any of the following standard values (in minutes): 15, (30), and 45. Default offset value is 30 minutes.

Configuring secure mode of operation

Use this procedure to configure the parameters used by either the primary or secondary NTP server in secure mode of operation.

Procedure steps

Step	Action
1	Login to LD 117.
2	Enter the IP address(es) of the connected NTP server(s) as well as the Key ID. **CHG NTP SECURE PRIMARY/SECONDARY <key id>** The system prompts for the private key.
3	Enter the private key.
4	Confirm the private key.

ATTENTION

For security reasons, the private key does not show in the command line as you enter it.

—End—

Procedure job aid

Field	Description
PRIMARY/SECONDARY	Enter the server whose secure mode parameters you want to configure: Primary or Secondary.
<key id>	Enter the four digit Key ID. The default unassigned Key ID is 0.

Enabling secure mode of operation

Use this procedure to configure the mode of NTP operation to secure.

Prerequisites

- Configure the parameters for secure mode *before* enabling the mode of operation. See "Configuring secure mode of operation" (page 76).
- For both primary and secondary servers to operate in secure mode, configure both servers for secure mode, then select **ALL** in this procedure.

Procedure steps

Step	Action
1	Login to LD 117.
2	Change NTP security mode of operation to secure. **CHG NTP AUTHMODE SECURE <PRIMARY/SECONDARY/ALL>**

—End—

Disabling secure mode of operation

Use this procedure to set the NTP security mode of operation to insecure.

Procedure steps

Step	Action
1	Login to LD 117.
2	Change NTP security mode of operation to insecure. **CHG NTP AUTHMODE INSECURE <PRIMARY/SECONDARY/ALL>**

—End—

Configuring UTC offset for local time zone

Use this procedure to set the offset value (from UTC) for the local time zone.

Procedure steps

Step	Action
1	Login to LD 117.
2	Enter the offset value for the local time zone. `CHG UTCOFFSET <+/-hh:mm>`

—End—

Job aid

Field	Description
`<+/-hh:mm>`	Enter the number of hours and minutes by which the local time zone differs from the UTC. The default offset value is `+00:00`.

Adjusting for Daylight Saving Time

Use LD 02 to configure the date and time you want the system clock to move forward for Daylight Saving Time, or backward to return to standard time. You can also enable automatic change to Daylight Saving Time. For more information about adjusting for Daylight Saving Time in LD 02, see *Software Input Output Administration (NN43001-611)*

Enabling NTP

Use this procedure to enable NTP.

Prerequisites

- Before you enable NTP, configure the IP addresses of the primary and, if necessary, secondary NTP servers. Failure to do so results in an error message.
- You can enable NTP with the following parameters configured to their default values:
  - mode of communication
  - threshold level
  - secure mode of operation
  - time interval
  - UTC offset

However, to change these default values, you must do so before enabling NTP. Once enabled, you cannot change any NTP parameters.

- You cannot enable NTP with the Network Time Synchronization (NTS) feature enabled. Disable NTS before enabling NTP. Failure to do so results in an error message.

Procedure steps

Step	Action
1	Login to LD 117.
2	To enable NTP, enter the following command: `ENL NTP`

—End—

Disabling NTP

Use this procedure to disable NTP.

Prerequisites

- You cannot disable NTP with automatic synchronization running in the background. To disable NTP, first stop the background synchronization. See "Stopping background synchronization" (page 80).

Procedure steps

Step	Action
1	Login to LD 117.
2	To disable NTP, enter the following command: `DIS NTP`

—End—

Synchronizing NTP to run in the background

Use this procedure to begin querying the NTP server in background mode.

Procedure steps

Step	Action
1	Login to LD 117.

2 Set synchronization to: background.

```
SYNC NTP BKGD
```

—End—

Synchronizing NTP manually

Use this procedure to query the NTP server manually.

Procedure steps

Step	Action
1	Login to LD 117.
2	Set synchronization to: manual. `SYNC NTP MANUAL`

ATTENTION

Manual synchronization places LD 117 on hold for 15 seconds. During that time, you cannot abort from the overlay.

—End—

Stopping background synchronization

Use this procedure to stop background synchronization from running. NTP remains enabled.

Prerequisites

- You cannot stop a background synchronization if no background routine is running. Attempts to do so result in an error message.

Procedure steps

Step	Action
1	Login to LD 117.

2	To stop the background routine, enter the following command:
	`STOP NTP BKGD`
	The system generates the following message asking you to confirm the operation:
	`NTP Query is being processed`
	`Do you want to proceed (y/n)?`

3 Enter `y`.

—End—

Checking NTP status

Use this procedure to verify the current NTP status.

Procedure steps

Step	Action
1	Login to LD 117.
2	To view NTP status, enter the following command: `STAT NTP`

—End—

Printing NTP parameters

Use this procedure to display the current configuration of NTP.

Procedure steps

Step	Action
1	Login to LD 117.
2	To display current configuration, enter the following command: `PRT NTP`

—End—

Feature implementation using Element Manager

Use these procedures to implement CS 1000 Network Time Protocol in Element Manager.

Prerequisites for implementing NTP using Element Manager

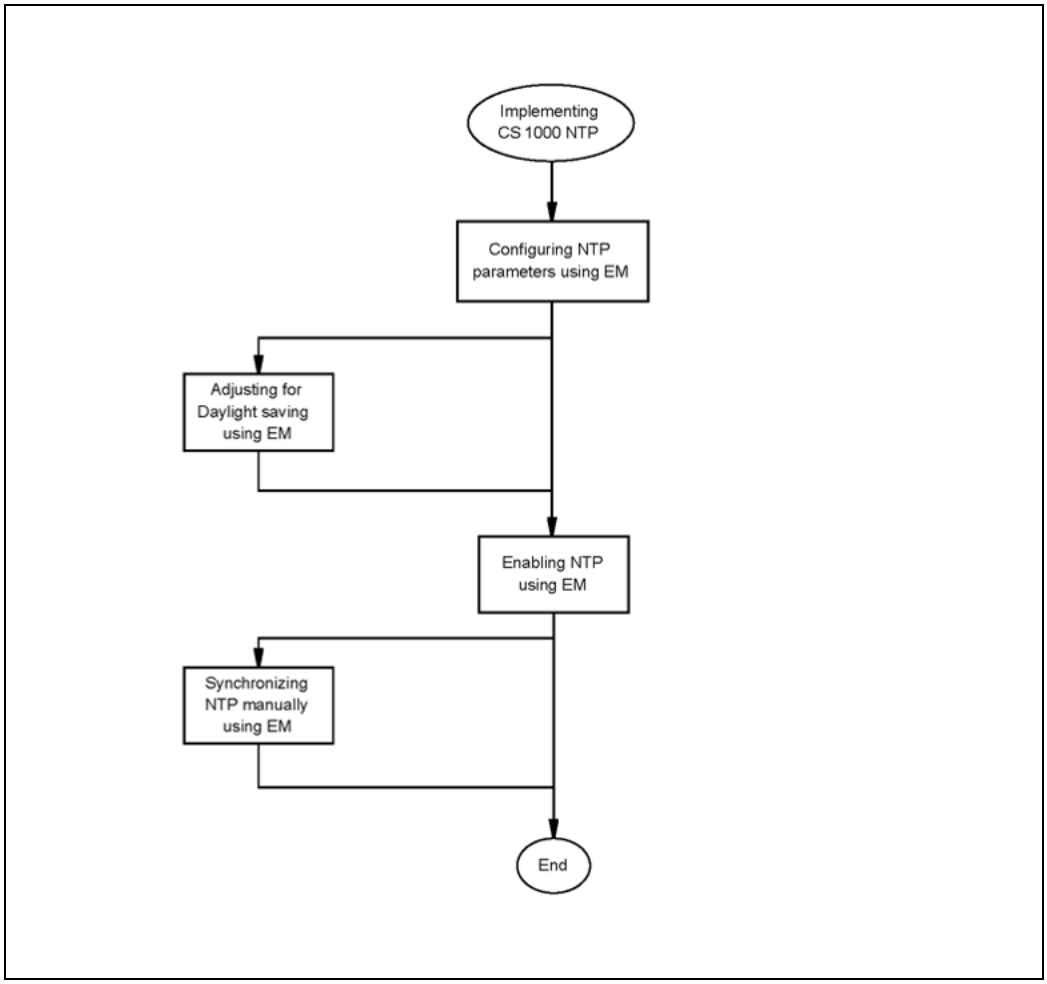
- You must have at least one NTP server available to the system.
- For full access to NTP configuration from Element Manager, login with Level 2 user status. If you login without Level 2 status, Element Manager displays an error message.

- Before you start, obtain the IP addresses for your primary and (if included on the system) secondary NTP servers.

Procedures for implementing NTP using Element Manager

This task flow shows the sequence of procedures performed to implement Network Time Protocol with Element Manager. To link to any procedure, see "Procedures for implementing NTP using EM" (page 82).

Figure 5
Implementing CS 1000 NTP using Element Manager



Procedures for implementing NTP using EM

- "Configuring NTP parameters using EM" (page 83)
- "Adjusting for Daylight saving using EM" (page 84)
- "Enabling NTP using Element Manager" (page 84)
- "Disabling NTP using Element Manager" (page 85)

- "Synchronizing NTP manually using Element Manager" (page 85)

Configuring NTP parameters using EM

Use this procedure to configure NTP parameters.

Procedure steps

Step	Action
1	Login to Element Manager.
2	Click **Tools > Date and Time**.
3	Click **Configure**.
4	Select mode of communication: **Call Server** or **Signaling Server**.
5	Select security mode: **Secure** or **Insecure**.
6	Enter the IP address of the primary NTP server.
7	If in secure mode, enter the **Key ID** and **Private Key** for the primary NTP server.
8	If the system includes a secondary NTP server, enter the IP address for that server.
9	If in secure mode, enter the **Key ID** and **Private Key** for the secondary NTP server.
10	To run NTP as a background process, check **Automatic Background Synchronization**.
11	If running NTP in the background, enter values for the **Polling Interval** and **Query Offset**.
12	Select the local time zone from the drop-down list.
13	Select values for the three threshold levels: **Normal**, **Warning**, and **Critical** (mandatory).
14	To complete the configuration, click **Save**.

ATTENTION

If NTP is already enabled, clicking **Save** disables NTP. To implement the feature, you must subsequently enable NTP. See "Enabling NTP using Element Manager" (page 84)

—End—

Adjusting for Daylight saving using EM

Use this procedure to change the daylight-saving parameters.

Procedure steps

Step	Action
1	Login to Element Manager.
2	Click **Tools > Date and Time**.
3	Check **Adjust for Daylight Savings**.
4	Use the drop-down menus to specify the date and time you want to move the clock forward one hour for Daylight Saving Time.
5	Use the drop-down menus to specify the date and time you want to move the clock backward one hour to return to regular time.
6	To complete the adjustment, click **Save**.

—End—

Enabling NTP using Element Manager

Use this procedure to enable NTP using Element Manager.

Prerequisites

- Configure NTP parameters before enabling NTP. See "Configuring NTP parameters using EM" (page 83).
- If you select Automatic Background Synchronization during NTP configuration, enabling NTP launches regular NTP time updates, according to the configured polling interval.

Procedure steps

Step	Action
1	Login to Element Manager as a Level 2 user.
2	Click **Tools > Date and Time**.
3	Click **Enable**.

—End—

Disabling NTP using Element Manager

Use this procedure to disable NTP.

Procedure steps

Step	Action
1	Login to Element Manager as a Level 2 user.
2	Click **Tools > Date and Time**.
3	Click **Disable**.

—End—

Synchronizing NTP manually using Element Manager

Use this procedure to manually synchronize with the NTP server. Manual synchronization does not interfere with automatic background synchronizations (background synchronization still takes place, at the configured time interval).

Procedure steps

Step	Action
1	Login to Element Manager as a Level 2 user.
2	Click **Tools > Date and Time**.
3	Click **Sync Now**.

—End—

Nortel Converged Office

The Nortel Converged Office Solution supports the following enhancements for Communication Server (CS) 1000 Release 5.0:

- Do Not Disturb: The “Do Not Disturb” feature is now offered through SIP CTI.
- Video Calls: Video calls are supported in the Microsoft Office Communicator to Office Communicator Session Initiation Protocol (SIP) Gateway call scenario.
- Transport Layer Security (TLS): TLS is now available in both SIP CTI and Nortel’s Multimedia Convergence Manager (MCM). TLS provides secure calls from Office Communicator to the CS 1000 call server.
- RFC2833: DTMF digits dialed from Office Communicator or an IP telephone on the CS 1000 are now sent using the RFC2833 standard.
- SIP Proxy Server (SPS): The Converged Office Solution can now work with either the new SPS or the legacy Network Redirect Service (NRS).
- DNS: The Signaling Server RadVision SIP Stack now supports Domain Naming Server (DNS) configuration. As a result, static Host Table configurations are no longer required in CS 1000 Release 5.0.
- Enhanced Security: SIP CTI now has an option that only accepts TLS end points. This feature enhances security by ensuring that only authorized hosts with TLS certificates can control a particular telephone.
- G.723: Both G.711 20 ms and G.723 are now supported in the Office Communicator to IP Phone call scenario.

The Nortel Converged Office Solution also introduces several user interface and serviceability enhancements to its MCM software in CS 1000 Release 5.0.

For more information about Nortel Converged Office, see: *Nortel Converged Office Fundamentals (NN43001-525)*.

Security and Emergency Services

The security enhancements in Communication Server (CS) 1000 Release 5.0 deliver new features that protect the system against intrusion or misuse, and protects information and voice traffic transmitted within or between systems. The enhancements include:

- "OAM security enhancements" (page 91)
- "Media Security" (page 92)
- "Intrasystem Signaling Security" (page 93)
- "Transport Layer Security for SIP" (page 93)
- "Secure signaling using SMC 2450" (page 93)Secure signaling using SMC 2450
- "Emergency Services Access" (page 95)

Security Enhancements

Overview

The following security features are new in Communication Server (CS) 1000 Release 5.0:

- Secure remote access is provided by Secure Shell (SSH).
- Security for individual call streams is provided by the Media Security feature.
- Security for ELAN subnets is provided by an Intrasystem Signalling Security (ISSS) solution based on the industry standard IP Security (IPsec).
- Security for SIP signaling is provided by Transport Layer Security (TLS).
- Security for data exchanges between the IP Phones and the Signaling Server is provided by Secure UNIStim signaling, which requires a Secure Multimedia Controller (SMC) 2450 device.

All of these enhancements work in conjunction with existing security features to provide a more complete security solution.

OAM security enhancements

The OAM Security enhancements improve the overall security of the system by providing a customizable logon banner, greater account management functionality, security event logging operations, remote shell access controls, and secure remote shell access.

For customers who have security policies that require network equipment to display a specific message to users when they log in, the customizable logon banner displays up to 20 lines of custom text.

Improved account management

Improved account management features include:

- password history and reuse controls are provided
- automatic password aging controls are provided

- every user can now change their own password
- user names are now required for all logons
- inactive accounts are automatically disabled
- inactive session logout controls are provided
- improved role management provides the ability to fully configure access privileges for individual users
- log on is now required to access the system, not merely to make changes

Improved logging

Security events are now logged with greater detail, including the following changes:

- remote host IP information
- more events are logged, including account modifications and secure configuration access requests
- security events are logged using the prefix "SEC" (such as SEC0001, SEC0002, SEC0003), making them easier to identify
- improved log display
- SNMP traps for security events
- improved accuracy of error logging
- logs and error reporting now survive system restart.

Tools and filtering capabilities are provided to view the logs.

Enhanced remote access security through SSH

Secure Remote Access is now supported using Secure Shell (SSH), which allows remote users to securely access the system and perform system operations. You can now disable access to any of the following:

- FTP access for end users
- secure remote shell access
- secure file transfer access for end users

Media Security

The Media Security feature provides a means by which two endpoints capable of Secure Real-Time Transport Protocol (SRTP) can engage in secure media exchanges. If Media Security is enabled, and an IP Phone is using SRTP to encrypt and authenticate the media stream, the system displays a security icon on the IP Phone. On some IP Phones, the message "encrypted" also appears.

Media Security uses a shared key to encrypt the media. The key is distributed over the SIP trunks, which rely on the SIP TLS feature for security. For more information about SIP TLS, see "Transport Layer Security for SIP" (page 93). For clients served by a common CS 1000 Call Server, the keys and cryptographic material are transmitted using UNIStim messages, which can be protected using the SMC 2450.

Intrasystem Signaling Security

The IP Security framework (IPsec) provides an Intrasystem Signaling Security (ISSS) solution that works with all IP protocols. IPsec works at a low layer of the network (Layer 3 of the OSI 7-Layer Model). This makes it possible for software applications to engage in secure communications without the addition of communications security code to each application.

The feature performs IPsec peer authentication using a preshared secret, and uses the Internet Key Exchange (IKE) protocol to automatically negotiate keying materials for data stream encryption between IPsec peers.

Transport Layer Security for SIP

Transport Layer Security (TLS) is used to secure SIP signaling traffic. SIP TLS provides message confidentiality and integrity, and it provides client-server authentication at the transport layer. SIP TLS protects communication between SIP endpoints by providing:

- Confidentiality: Symmetric cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated through the TLS handshake protocol.
- Integrity: Message transport includes a message integrity check using a keyed message authentication code (MAC). Secure hash functions are used for MAC computations.
- Authentication: If certificates signed by a trusted certificate authority (CA) are used, the client in a TLS connection can authenticate the identity of the server, and the server can optionally authenticate the identity of the client.

Secure signaling using SMC 2450

Secure UNIStim Signaling provides a means of encrypting data exchanges between the Signaling Server and IP phones. UNIStim signaling security is provided by the transparent UNIStim security proxy within the Secure Multimedia Controller (SMC) 2450. Secure UNIStim signaling enables UNIStim IP Phones to communicate with insecure UNIStim servers in a protected fashion, with encryption terminated at the SMC 2450 before the unencrypted traffic moves to the local server.

The SMC 2450 is a security system that creates a Secure Multimedia Zone (SMZ), protecting the SMZ from traffic on the enterprise LAN/WAN. All signaling and media traffic entering or leaving the SMZ must pass through the SMC 2450.

For more information

For more information about the features discussed in this chapter, see:

- *Security Management Fundamentals (NN43001-604)*
- *Secure Multimedia Controller Fundamentals (NN43001-325)*

For information about security features in the Enterprise Common Manager (ECM) security framework, including central authentication, user and role management, certificate management, and access control, see "Enterprise Common Manager" (page 169).

Emergency Services Access

The Emergency Services Access feature has been developed to extend location-based handling of ESA emergency calls to all connected telephony clients (especially IP Phones, but also to non-IP telephones, for which precise caller location has been previously difficult to determine.

IP telephony clients, for example, are not restricted to making connections using a fixed port; they can connect to a Call Server from any port currently active on the network. Therefore, they are easily relocated from one network port to another without following an administrative process. In addition, IP Phones can also be nomadic or mobile if they utilize a wireless handset, or if they are installed as part of a Virtual Office scenario. The problem caused by the resulting “client mobility” is that if an emergency caller’s specific location cannot be determined, effective emergency call handling is not possible.

CS 1000 Release 5.0 Emergency Services Access introduces Location Management functionality. This functionality allows for the determination and subsequent management of the current location information for an emergency caller, even if they are using a mobile phone type for which location determination has traditionally been an issue. In this way, ESA emergency call handling is delivered for the precise location of the caller, making existing emergency coverage more effective.

Several other improvements are introduced to emergency call handling, through the introduction of several additional enhancements to the existing ESA implementation. These are summarized as follows:

- Emergency location-based emergency call treatment is now possible for all telephones connected to the enterprise network, regardless of phone type.
- In CS 1000 Release 5.0, CLID composition is enhanced to allow for more flexibility in assigning an ESA CLID to an emergency caller. An Emergency Location Identification Number (ELIN) can now be dynamically assigned to a telephone that cannot use its Direct In Dial (DID) number as its Caller ID. The ELIN provides a usable Caller ID (CLID) to the responding Public Safety Answering Point (PSAP) that allows a callback to be made directly to the emergency caller, which

could not previously have been done. This feature applies to both IP Phones and non-IP telephones.

- Support for the use of Route List Indexes (RLIs) is introduced, which allows ESA to identify alternate routing for emergency calls, in the event that the standard route is unavailable. This functionality helps to ensure that an emergency call receives emergency handling by ensuring delivery of the call to the appropriate emergency responder, including the ability to locally terminate an ESA call without required use of loopback trunks.
- On-Site Notification (OSN) output and SNMP traps are enhanced to provide more detailed emergency call information.
- Virtual Office ESA calls can now route directly to the host Call Server for emergency call handling, rather than being redirected.
- Support is introduced for Multiple ESDN. Previously, it was only possible to configure a single ESDN to be used in placing emergency calls. With CS 1000 Release 5.0 ESA, it is possible to configure up to 16 distinct ESDNs to better suit the needs of a multinational enterprise.
- Implementation of the Misdial Prevention functionality, which provides system administrators with the ability to prevent ESA calls from being made due to an accidentally misdialed ESDN. Cases outlining possible ESDN misdials can be configured for each ESDN entry in use in the enterprise (a notification is made for all calls blocked in this fashion, using the Misdial Prevention functionality).

In addition to the enhancements made to the basic Emergency Services Access feature, CS 1000 Release 5.0 introduces further feature functionality enhancements to ESA by means of the ***Emergency Services Networked M911 Operation*** and ***Basic Emergency Services When VO Logged Out*** features, as described in the following sections:

Emergency Services Networked M911 Operation

The Emergency Services Access (ESA) feature does not currently support direct tandem routing of E911 calls from one CS 1000 Call Server to another. Post September 11, 2001, it has become apparent that survivability of a Public Safety Answering Point (PSAP) based on geographic distribution is the key to providing critical public safety services. The Emergency Services Networked M911 Operation feature adds functionality to the current ESA implementation, so that emergency calls can be tandem transferred from one CS 1000 to another in an MCDN environment, and receive full emergency call treatment regardless of call origin.

The Emergency Services Networked M911 Operation feature supports the following, in addition to those currently supported by basic ESA:

- A new trunk sub-type, M911P, is introduced exclusively for tandem routing of E911 calls over TIE trunks.
- Network ACD/Network Skill Based Routing and Call Abandon functionality – this functionality ensures that a tandem routed E911 call is handled appropriately at the target Call Server.
- 10/20 digit ANI support
- Malicious Call Trace – In the event that an emergency call must be traced while a 911 call is in progress, activation of this feature can identify the trunk by which the E911 call is being routed
- Centrex Hook Switch Flash capability over 911P trunks to support call transfer on a Selective Router.

Basic Emergency Services When VO Logged Out

Prior to this feature being introduced, logged out IP Phones could not be used for basic telephony function - making and receiving calls. The reason was that basic telephony functions were controlled by the central Call Server.

CS 1000 Release 5.0 introduces the ability for the logged out phones to make Emergency Services Access (ESA) calls and receive callbacks, by temporarily registering IP Phones with the Call Server.

The *Basic Emergency Services When VO Logged Out* feature provides a base level of service for the logged out IP Phones. This base level of service allows VO logged out IP Phones to utilize emergency services. Features such as transfer, conference, re-dial, mail box, or directory, are not provided to the IP Phone.

The permitted outgoing calls include any of the provisioned ESDN numbers.

Business Continuity

The following enhancements and support delivers Business continuity improvements from a reliable and resilient environment:

- "IP Line 5.0 feature enhancements" (page 101)
- "Context-sensitive soft keys" (page 109)
- "CLID Name Enhancement" (page 119)
- "ISDN CLID Enhancement" (page 139)
- "Bandwidth Management Support for Network Wide Virtual Office" (page 155)
- "Network Music" (page 157)

IP Line 5.0 feature enhancements

Description

Communication Server (CS) 1000 Release 5.0 introduces the following enhancements:

- "New IP Phone Types" (page 101)
- "New languages and Unicode support" (page 104)
- "IP Client cookies" (page 107)
- "Live Dialpad" (page 108)

New IP Phone Types

CS 1000 Release 5.0 introduces the New IP Phone Types feature which adds new TN types to the Call Server and Line Terminal Proxy Server (LTPS) software.

Description

The New IP Phone Types feature introduces the following:

- unique TN types for each IP Phone
- emulation mode for IP Phones which are not known by the TPS but have the same capabilities as the IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Softphone 2050, or IP Phone 1150E
- automatic and manual IP Phone TN type conversion
- enhanced Model Names support so that Model Name information is accessible from LD 20 and Telephony Manager 3.1.

Unique TN types for each IP Phone The names of existing IP Phone TN types are updated with the new IP Phone naming convention.

Table 4 "CS 1000 Release 5.0 TN type naming convention" (page 102) shows the unique IP Phone TN type naming convention for CS 1000 Release 5.0

Table 4
CS 1000 Release 5.0 TN type naming convention

IP Phone model name	CS 1000 Release 4.5 TN_TYPE	CS 1000 Release 5.0 TN_TYPE
IP Phone 2001	i2001	2001P2
IP Phone 2002 Phase I	i2002	2002P1
IP Phone 2002 Phase II	i2002	2002P2
IP Phone 2004 Phase 0/1	i2004	2004P1
IP Phone 2004 Phase II	i2004	2004P2
IP Audio Conference Phone 2033	i2001	2033
IP Softphone 2050	i2050	2050PC
Mobile Voice Client 2050	i2050	2050MC
WLAN Handset 2210	i2004	2210
WLAN Handset 2211	i2004	2211
WLAN Handset 2212	i2004	2212
IP Phone 1110	i2001	1110
IP Phone 2007	i2004	2007
IP Phone 1120E	i2002	1120
IP Phone 1140E	i2004	1140
IP Phone 1150E	IPACD	1150

Emulation Mode During IP Phone registration, the LTPS determines the IP Phone TN type (TN_Type) by looking up its User Interface capabilities (UI_TYPE) and firmware ID (FW_ID) in a mapping table. The mapping table is used to map the IP Phone UI_TYPE, FW_ID , with the TN_TYPE. If an IP Phone has known UI_TYPE but an unknown UI_TYPE and FW_ID combination, the IP Phone is registered in Emulation Mode. Use the isetShow command or LD 20 to list the IP Phones registered in Emulation Mode. The isetShow command lists the IP Phones registered in emulation mode marked with EM next to their TYPE. LD 20 Print Routine 1 prints EMULATED after the TN type indicating the IP Phone is registered in Emulation Mode.

Automatic IP Phone TN conversion (Flexible Registration) CS 1000 Release 5.0 introduces Flexible Registration Class of Service (CLS) for all IP Phones. Flexible Registration can be set to one of the following values:

- FRA—Flexible Registration Allowed (default)
- FRU—Flexible Registration on Upgrade
- FRD—Flexible Registration Denied

Use LD 81 to list the IP Phone TNs which have FRA, FRU, and FRD class of service set.

When the LTPS attempts to register an IP Phone with the Call Server, the following takes place:

1. If the TN has FRD class of service, the Call Server checks the IP Phone type against the TN type. Registration is rejected if the types do not match. Furthermore, the Call Server checks the Emulation Flag and blocks registration in Emulation Mode.
2. If the TN has FRA class of service, the Call Server checks its compatibility table to find out if the IP Phone is compatible with the TN type. If the types are compatible, the TN is converted and the IP Phone registers.
3. If the TN has FRU class of service, the Call Server checks its compatibility table to find out if the IP Phone is compatible with the VTN type. If the types are compatible, the TN is converted and the IP Phone registers. After the TN is converted, the Flexible Registration class of service is set to FRD. The Call Server checks the Emulation Flag and blocks registration in Emulation Mode.

In the case of FRA and FRU, an additional check for KEM compatibility is performed. If the TN has KEM(s) configured and the registering IP Phone does not support a KEM (due to lack of Accessory Expansion Module, or a limited display area) the registration is rejected.

Manual IP Phone TN conversion Manual IP Phone TN conversion lowers the administrative effort required to replace an IP Phone with another model while preserving the IP Phone features. CHGTYP is a new response added to the REQ prompt in LD 11 to convert any IP Phone TN to any other IP Phone TN while restricting unsupported features.

Table 5 "Command definitions in LD 11" (page 104) shows command definitions in LD 11

Table 5
Command definitions in LD 11

Prompt	Response	Description
REQ	CHGTYP	Change type of an IP Phone TN
TYPE	2004P1, 2004P2, 2002P1, 2002P2, 2001P2, 2050PC, 2050MC, 2033, 2210, 2211, 2212, 1110, 2007, 1120, 1140, 1150	Specifies the type of TN block to convert
TN	l s c u for Large Systems c u for Small Systems	Specifies the TN to convert
NEWTYP	2004P1, 2004P2, 2002P1, 2002P2, 2001P2, 2050PC, 2050MC, 2033, 2210, 2211, 2212, 1110, 2007, 1120, 1140, 1150	Specifies the TN_TYPE to convert The Call Server lists the features that will be lost.
PROCEED	YES NO	Confirms that the system administration is aware of what features will be lost and still wants to perform the conversion.

Model Names Model Names are fully supported for IP Phones. Model Names enable you to determine the following:

- the IP Phone model registered in Emulation Mode
- the IP Phone model when the names of TN types no longer match the model names of the IP Phones (future rebranding)

New languages and Unicode support

CS 1000 Release 5.0 introduces the following language enhancements for the IP Phone 2007, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E:

- UNIStim font messages interpreted as UTF-8— enables the Call Server to easily display complex fonts, such as Arabic, Simplified Chinese, Traditional Chinese, Japanese, and Korean on an IP Phone.
- Support for TFTP Server—an extension of the existing configuration file is used to download fonts as needed into the IP Phone.

- Synchronization of the display language between the Call Server and the IP Phone—local prompts on the IP Phone and text from the Call Server are displayed in the same language.

UNIStim font messages interpreted as UTF-8

UTF-8 is used as character encoding between the Call Server and the IP Phone. This must be enabled on the Call Server in order for the fonts to be downloaded. After the Call Server has downloaded the appropriate fonts, the IP Phone can display all languages for which it has appropriate character sets. Although the IP Phone supports the languages for which it has appropriate character sets, only one language can be displayed at a time.

TFTP Server support

A configuration file is used to download font files, as needed, to the IP Phone using a TFTP Server. After the font files are downloaded to the IP Phone, the configuration file creates a mapping, so the IP Phone knows how and when to use the font.

Synchronizing the language

If the Call Server initiates a language change, the IP Phone changes its local prompts to match the specified language on the Call Server. If the IP Phone user initiates a language change using the Local Tools menu, the Call Server changes its local prompts to match the specified language on the IP Phone. If the Call Server selects a language which the IP Phone does not support, the local prompts default to English.

Expansion Module for IP Phone 1100 Series font support

The Expansion Module for IP Phone 1100 Series (Expansion Module) text is rendered by the IP Phone; therefore, the selected language and font mappings on the Expansion Module mirror the selected language and font mappings on the IP Phone.

Downloading and configuring fonts

The font files are downloaded as needed using the same TFTP Server configuration file method as IP Phone 2007, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E.

The IP Phone downloads the required files specified in the configuration file, as necessary. The following table describes the fields in the configuration file on the TFTP Server for downloadable fonts. The section [FONTxx] indicates the font file. Set the download mode to AUTO or FORCED. Nortel recommends that you set DOWNLOAD_MODE to AUTO.

Table 6
TFTP configuration file

Field Name	Field Value	Description
[FONTxx]		Section header for the font file, which contains font information, including the optional download parameters, versions, and how to use the font after it is downloaded. Only [FONT01] to [FONT10] are supported.
DOWNLOAD_MODE	AUTO	Recommended setting. The application looks at the version and downloads the font if it is a newer version than the one on the IP Phone.
	FORCED	The version of the font is ignored. The configuration file is always downloaded.
PROTOCOL	TFTP	Download protocol. Must be TFTP.
SERVER_IP	xxx.xxx.xxx.xxx	IP Address of the TFTP server in decimal.
SECURITY_MODE	0	For future use.
FILENAME		Image file name. Must match the file name of the actual IP Phone FW file.
ALIAS		Enables the font to have a different name in the IP Phone file system than the one on the Call Server.
VERSION		The version string compared to what is on the IP Phone.

FONTLANG		Configuration command that defines the language codes for which a font is used. FONTLANG = languagelist Where: languagelist is a comma separated list of ISO 639-2/RFC 3066 codes. See the Display Manager Assign IT Language UNIStim message for details on language codes.
MAP		Configuration command that defines how the font is mapped in the Unicode character set. MAP xx xx xx xx xx xx xx xx xx xx Where: xx…xx = 10 hex bytes defining the ulUnicode ranges for a font in the same format as the IT Character Set Report.

IP Client cookies

IP Client cookies provide a transparent transfer of data from the Call Server to third-party applications; for example, Citrix AG. The cookies are a set of UTF-8 variable names and values which are duplicated and synchronized between the LTPS and the IP Phone. IP Line 5.0 uses public cookies which are visible to both the IP Phone and third-party applications.

The following IP Phones support IP Client cookies:

- Phase II IP Phones
- IP Phone 2007
- IP Phone 1110
- IP Phone 1120E
- IP Phone 1140E
- IP Phone 1150E

IP Client cookies are not supported on Phase I IP Phones, IP Phone Audio Conference Phone 2033, and WLAN Handsets 2210/2211/2212/6120/6140.

Table 7
Cookie definitions

Cookie name	Description
PrimeDN	A string of digits containing the current primary DN of the IP Phone.
AgentPosition	A string of digits containing the current agent position of the IP Phone. This string is empty if the agent is not logged in.
CallState	A UTF-8 string indicating the current call processing state of the IP Phone. The following are possible values: • BUSY-an active call is established • IDLE-no active calls (there can be calls on hold) • RINGING-IP Phone is ringing
CustNo	A string of digits indicating the IP Phone customer number.
Zone	A string of digits indicating the IP Phone zone.
VPNI	A string of digits containing the Virtual Private Network Identifier configured for the IP Phone.
TN	UFT-8 string containing the TN currently associated with the IP Phone in hexadecimal format. The maximum number of TNs is FFFF.
Although cookie names and values are UTF-8 strings, it is not necessary for the IP Phone to support Unicode.	

Live Dialpad

CS 1000 Release 5.0 introduces the Live Dialpad feature for IP Phones. The primary Directory Number (DN) key is activated when the user makes a call by dialing a DN on the dialpad without picking up the handset or pressing the Handsfree key. To set the Live Dialpad feature to On or Off, select **Telephone Options > Live Dialpad**. By default, Live Dialpad is set to Off.

Context-sensitive soft keys

Feature description

Context-sensitive soft keys provide dynamic functionality to the IP Phones similar to that currently supported on the M39xx digital telephone series.

Context-sensitive soft keys are located directly below the LCD screen on the IP Phone. The soft key label above each key dynamically changes depending on the call processing state.

Two new soft keys, Callers List and Redial List, appear in the default idle state when an IP phone is registered on a Signaling Server with Personal Directory (PD) server enabled.

The Call Server adds up to ten additional Context-sensitive soft keys on the IP Phones. See Table 9 "Call features" (page 110) for a list of the call features with its corresponding soft key position. The functionality and labeling of soft keys on an IP Phone is defined by the Call Server using the key map download message. The context-sensitive soft key feature is enabled on the IP Phone and cannot be turned on or off.

See "Using call features" (page 114) for examples of IP Phone screens in different call states.

Soft keys configuration

The default order and position of the soft keys change depending on the features that are configured by a system administrator. For each feature that is not configured, the corresponding soft key does not appear in the applicable screen. If a soft key is not configured, the remaining soft keys shift up to fill the empty soft key position.

The set of soft keys must be configured in set data block for IP terminal in LD 11.

Table 8
LD 11 - Configure soft keys

Prompt	Response	Description
REQ	NEW	Configure a new soft key
TYPE	xxxx	Type of telephone
CUST	xx	Customer number
TN		
...		
...		
KEY	x aaa yyy (cccc or D)	xx = Key number aaa = Key name or function (SCR/MCR/PVN/PVR/SCN yyyy = DN cccc = CLID table entry of (0)-N, where N = the value entered at the SIZE prompt in LD 15 minus 1. D = the character "D". When the character D is entered, the system searches the DN keys from key 0 and up to find a DN key with a CLID table entry. The CLID associated with the found DN key is then used.
...		

Table 9
Call features

Key Number	Feature Name	Description
17	Call Transfer (TRN)	Use the Call Transfer feature to transfer a call to a third-party. You can consult with the third-party privately before completing the transfer.
18	Three-party conference (A03) or Six-party conference (A06)	The conference feature adds additional parties to an established call. The maximum is three or six, depending on the conference feature assigned to the conference call originator. A system administrator manually configures the feature for Three- or Six-party conference call using LD 11.

Key Number	Feature Name	Description
19	Call Forward (CFW)	Call Forward automatically forwards incoming calls to another destination, within or outside the system.
20	Ring Again (RGA)	After a busy tone is received, the Ring Again feature alerts the caller once the line becomes free.
21	Call Park (PRK)	Call Park places a call in a parked state, similar to hold, where it can be retrieved by an Attendant Console or telephone. A parked call must have an access ID, also known as a Park DN.
22	Ringing Number Pickup (RNP)	An incoming call on one telephone can be picked up on another telephone. A system administrator defines the call pickup group.
23	Speed Call (SCU/SCC) or System Speed Call (SSU/SSC)	A call is made using a one-, two-, or three-digit code. Your system administrator defines the Speed Call code and Speed Call lists. ***Note:*** The soft key label on your telephone can appear as **`SpcUsr`** or **`SpdCtl`** depending on how Key 23 in LD 11 is defined by your System Administrator.
24	Privacy Release (PRS)	In multiple appearance, single call arrangements, the Privacy Release feature allows another appearance of the Directory Number (DN) to enter the call. Privacy is then reestablished until Privacy Release is activated again.
25	Charge Account (CHG)	After a Charge Account number is used, the entire call is billed to that DN. The number can be entered before or during a call. The Charge Account feature is not supported for internal calls.
26	Call Party Number (CPN)	This feature is used in conjunction with Call Detail Recording (CDR). A Charge Account call is billed directly to a specific account or charge number instead of a DN.

Operating parameters

Features are added or removed by a system administrator using LD 11. The default order and position of soft keys is determined by the number of features configured on your IP Phone.

The following IP Phones support the context-sensitive soft key feature:

- IP Phone 2001

- IP Phone 2002 and 2004—Phase II
- IP Phone 2007
- IP 2050 Softphone
- IP Phone 1110, 1120E, 1140E, and 1150E
- IP Phone 2033
- WLAN Handsets 2210, 2211, and 2212

Feature restrictions

Context-sensitive soft keys are supported on the Survivable Remote Gateway (SRG) in normal mode only.

Feature interactions

When the Context-sensitive soft keys on the IP Phone are used by a Call-Server-based application such as Corporate Directory or a Signaling Server-based application such as Personal Directory, the soft keys are defined by the active application. The application controls the soft labels that are displayed. The IP Phone returns to the Context-Sensitive Soft Key labeling upon completion of the application.

During an abnormal call-processing operation, the IP Phone advances to the Reorder state screen and the Reorder tone is sounded. For example, if an invalid extension is entered, the Reorder state screen appears on the display with the message **`Release and try again.`**

CallPilot-related soft keys are only available if the CallPilot voice mailbox is accessed from an IP Phone by using the inbox key instead of directly dialing a CallPilot DN.

The IP Phone 2033 and some third-party IP Phones have only three soft keys . The firmware handles the translation from four soft keys to three soft keys.

Feature packaging

The Context-sensitive soft key feature is included in the base system software.

Feature implementation

The features listed in the "Soft keys configuration " (page 109) list can be added or removed by a system administrator using LD 11.

The Callers List and Redial List feature keys are not configurable in LD 11 because the Personal Directory feature is not a Call-Server-based application. These keys are available from the call-processing default idle state of the IP Phone if the Personal Directory (PD) server is enabled.

Feature operation

The following table identifies what is displayed on the IP Phone LCD screen when in a specific call state.

Table 10
Call state screens

Call state	Action	Display
Default Idle	Key map download message is sent to the telephone and the default idle state appears.	For IP Phone 2001, 2002, 1110, 1120E, and 2033, the default idle state is **`Fwd Caller Redial`** For IP Phone 2004, 2007, 2050, 1140E, and 1150E, the default idle state is **`Forward Callers Redial`** For WLAN Handsets 2210, 2211, and 2212, there are only four characters available for each soft key label. ***Note:*** Depending on your telephone type and the number of characters available for each soft key label on the LCD screen, some soft key labels can appear differently than what is identified in this document. For example, **`Forward`** appears as **`Fwd`** on an IP Phone 2001 with a six- character soft key label.
Dial Tone	Lift the handset or press the line (DN) key to get a dial tone. The dial tone screen appears.	**SpcUsr Pickup Charge CParty**
Predial	Press the dialpad from the idle state to advance the display to the predial screen.	**`CLEAR DELETE CANCEL`**
Dialing	There are no soft keys needed.	Extension number is displayed.
Ringing	The calling telephone receives ringback tone from the called telephone.	Extension and calling name are displayed. For example, **`7466 John Smith`**

Call state	Action	Display
Busy	If the destination number is busy, the display advances to the busy state screen.	**Destination Busy** **Activate RING AGAIN?** **RingAgn**
Reorder	If an invalid number is dialed, the reorder state screen appears.	**Release and try again**
Established (Active) Call	After a call is established there are two layers of soft keys available. Press the **More** key to toggle between these layers.	Layer 1: **Conf Trans Park More...** Layer 2: **PrivRls Charge CParty More...**

Note: Some soft keys such as the **SpcUsr** key are not configured by default. The System Administrator will configure as needed.

Using call features

Table 11
Examples of IP Phone screens in different call states

Feature	Action	Display
Call Forward	Press the **Forward** key from the default idle state.	**Enter Forward Number** appears on the display line.
Call Forward Number Edit	Enter the forward number.	**CFWD** **Press CFWD or Enter new #** The arrow continues to flash until you press the **>Forwar** soft key. The telephone is returned to the default idle state of **>Forwar Callers Redial** with an arrow beside **>Forwar**
Cancel Call Forward	Press the **>Forwar** soft key from the idle screen state.	**Call Forward cancelled**
Busy	A busy tone is received.	**Destination Busy** **Activate RING AGAIN?** ***Note:*** The Ring Again feature times out if the feature is not activated. The telephone returns to the idle state.
Ring Again Activate—screen 1	Press **RingAgn**.	**>RingAg Forward Callers Redial**

Feature	Action	Display
Ring Again Activate—screen 2	After the busy party is free, the IP Phone sends a short alerting tone.	**Ring again ready, Select a line RING AGAIN** **>RingAg Forward Callers Redial**
Cancel Ring Again	Press the **>RingAgn** soft key to cancel and return to the idle state.	**Forward Callers Redial**
Conference (available from the Established (Active) call state)	Press the **Conf** soft key.	The conference transfer dial tone screen appears: Layer 1: **>Conf SpcUsr Pickup More...** Layer 2: **Charge CParty More...** Enter a number. After the call is answered, press the **>Conf** soft key.
Transfer	Press the **Trans** soft key.	The transfer number editing state screen appears: Layer 1: **Trans SpcUsr Pickup More...** Layer 2: **Charge CParty More...** Enter a number and press the **>Trans** key for the telephone to return to the idle state screen.
Speed Call	From the dial tone state, press the **SpcUsr** soft key. ***Note:*** How this key is configured in LD 11 determines whether you see **SpcUsr** or **SpdCtl.**	Press the **SpcUsr** soft key. Enter the speed call code. The telephone advances to the ringing state.
Callers	Press the **Callers** soft key from the idle screen state. Press the up or down arrow on the telephone dialpad.	**Dial Edit Copy Del** appears on the screen
Redial	Press the **Redial** soft key from the idle screen state. Press the up or down arrow on the telephone dialpad.	**Dial Edit Copy Del** appears on the screen

Note: The IP Phone must be registered on the Signaling Server with the Personal Directory (PD) server enabled for the Callers and Redial soft key features to be available. The function of the Callers and Redial list views are controlled by the PD server which can be configured in LD 117.

CallPilot voice-mailbox-related soft keys

The following table identifies the soft keys in CallPilot as they relate to the IP Phone dialpad. CallPilot soft keys can be used instead of the telephone dialpad.

Note: CallPilot-related soft keys are only available if the CallPilot voice mailbox is accessed from an IP Phone by using the inbox key instead of directly dialing a CallPilot DN.

Table 12
CallPilot voice-mailbox-related soft keys

Feature	Action on CallPilot	Equivalent on telephone
Layer 1:		
Play	Press the **Play** key to listen to a message.	Press 2 on the dialpad.
Delete	Press the **Delete** key to delete the current message.	Press 7, 6 on the dialpad.
Call	Press the **Call** key to call the sender of a message.	Press 9 on the dialpad.
More...	Use the **More** key to toggle to layer 2.	
Layer 2:		
Stop	Press the **Stop** key to pause playback of a message.	Press # on the dialpad.
Conference	Press the **Conf** key to conference another caller to your voice mailbox. ***Note:*** This is not a CallPilot soft key but a Call Server feature key. This feature gives someone else access to your mailbox.	
Reply	Press the **Reply** key to the message.	Press 7, 1 on the dialpad.
More...	Use the **More** key to toggle to layer 3.	
Layer 3:		
Compose	Press the **Compose (Comp)** key to compose a new message.	Press 7, 5 on the dialpad.
Forward	Press the **Forward (FORWRD)** key to forward a message.	Press 7, 3 on the dialpad.

Feature	Action on CallPilot	Equivalent on telephone
Goodbye	Press the **Goodbye (Bye)** key to exit the voice message system.	Press 8, 3 on the dialpad.
More...	Use the **More** key to toggle back to layer 1.	

CLID Name Enhancement

Feature description

The Calling Line Identification (CLID) name enhancement introduces an enhancement to the existing functionality of name delivery for off-net calls. The CLID Name Enhancement feature provides an option for configuring and sending a group name when the calling party makes a call to the public network.

With this feature, different main numbers with different company names can be sent from the same PBX for some selected calls going over a public network (off-net calls). The name and extension of the user can be sent on calls going over a private network (on-net calls). As well, all the users of a single node can be grouped under one or more common groups and the group name is sent to the called node.

The group name is configured in the customer data block of the user and the group name of the caller is sent over public networks.

Before the enhancement, the Directory Number (DN) of the caller had a name attached to it and this name and number was sent with all calls, whether the call was on-net or off-net. With this feature enhancement, if the user makes an off-net call, the configured group name is sent. If the user is making a call on-net, the private name and number of the caller is sent.

With the CLID Name Enhancement feature, the following can be sent:

- different main numbers with different company names from the same PBX for selected off-net calls
- the name and extension of a user who is calling on-net.

This feature enhancement is particularly useful for the grouping of all users of a single node under a common group. The group name is sent to the called node.

The CLID Name Enhancement feature is applicable for Integrated Services Digital Network (ISDN) trunks that support name display. This feature is also applicable for Internet Protocol (IP) and Basic Rate Interface (BRI) trunks.

Feature restrictions

The feature enhancement depends upon the:

- Type of Number (TON)
- Numbering Plan Indicator (NPI) of the telephone making the call
- Capability of the telephone receiving the call

SL1, QSIG, EURO, NI2, D100, D250, and SL100 are the applicable interfaces that support name display, based on the TON and the NPI. All the privacy options available for the private name are supported for group name as well. This enhancement is a global feature that supports all ISDN interfaces that support name display. CLID Name Enhancement is not packaged.

Group name is not supported for originally called name and redirecting name.

CDP and UDP dialing plans continue to support private names with default CTYP in the DMI table and are, therefore, not supported.

If the originating call between two private networks is transferred over the public network, the final call does not involve any group names.

This table explains the TON and the NPI combinations that support group name. All other combinations of TON and NPI do not support group name.

Table 13
TON and NPI combinations that support group name

TON	NPI
International	E.164/E.163
National	E.164/E.163
Local	E.164/E.163
SPN	Private

Hardware and firmware are not affected by this feature enhancement. The following software components are affected:

- Service LD 95 Calling Party Name Display (CPND)
- Call-control modules for building the group name
- Conversion that allows sites to be upgraded to the new software release without manual service change and also maintain existing CLID capabilities
- Date required for the CLID table and the CLID entries

The CLID Name Enhancement feature handles the storage, building, and transportation of the caller's group name over a public network where TON and NPI are International /National and E.164/E.163, or SPN and Private.

The feature is operational for calling, connected, and alert or redirection of names only.

The feature works when public calls originate using SL1 and QSIG interfaces using the National Numbering Plan (NPA) or the Central Office Code (NXX) or SPN dialing plans based on the TON and NPI values that support the group name.

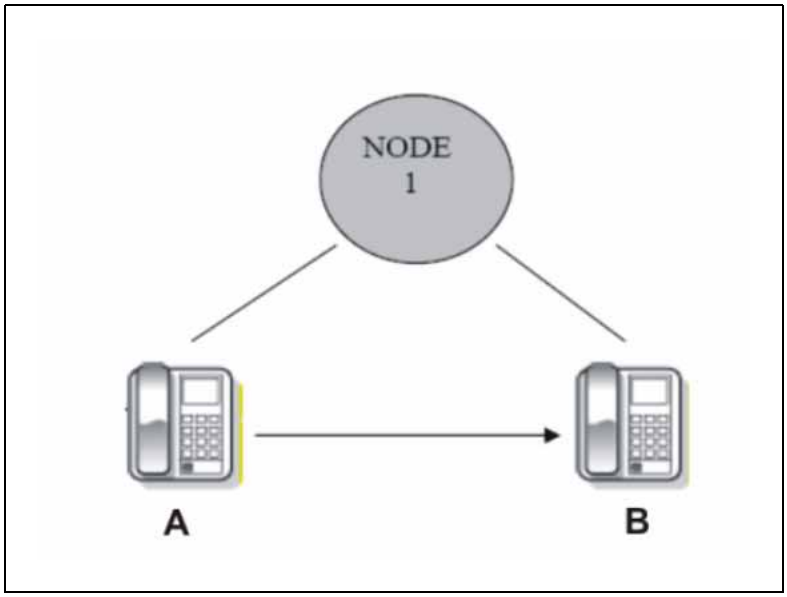
The name presentation indicator of the group name is based on the class of service, Name Presentation Denied (NAMD) or Name Presentation Allowed (NAMA), configured for the associated DN.

Group level options are allowed with this feature enhancement. A group name can be configured and sent as a generic name instead of sending a DN-based name during public calls. The group name is defined in the CLID entry associated with the DN. If there is no entry, the default CLID entry value zero is associated to the DN and the corresponding group name, if configured, is sent, or else the private name is sent.

Sample Scenarios

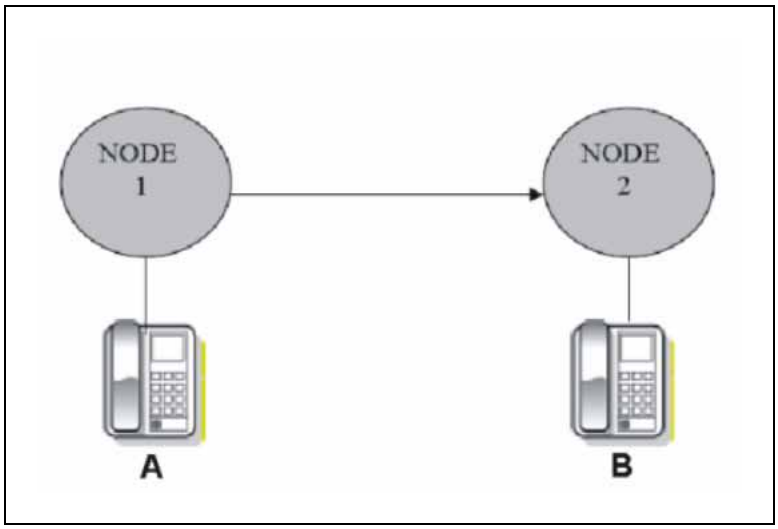
The tables in this section describe sample scenarios and the effect of the feature enhancement on the calls. Unless indicated, all nodes are CS 1000. The full capability of the sample scenarios can only be reached if CS 1000 is in use by both the telephone used in making the call and the telephone receiving the call.

Figure 6
General setup: One node, two telephones, A and B.



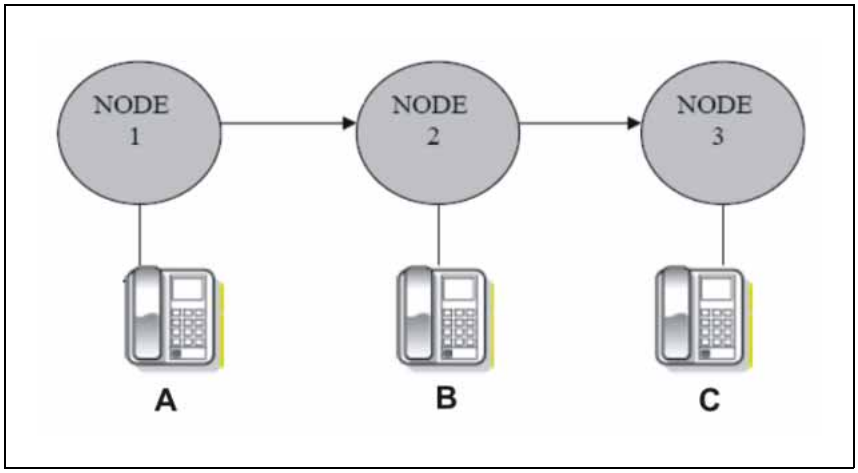
Type of call	Previous configuration	Previous scenario	Change in configuration with CLID name enhancement	Change in outcome of scenario with CLID Name Enhancement
On-net	The feature enhancement does not affect on-net calls. The same number is sent as before the CLID Name Enhancement.			

Figure 7
General setup: Two nodes, two telephones, A and B. Telephone A is on one node and telephone B is on the other node.



Type of call	Previous configuration	Previous scenario	Change in configuration with CLID name enhancement	Change in outcome of scenario with CLID Name Enhancement
Outgoing, off-net. Two nodes connected over a public network, over an interface that supports name display.	LD 11 or LD 95: CPND-NAME for each telephone	Telephone A (private name A) calls B (private name B). Telephone A sends its private name (A) to telephone B.	Same as before, except in LD 95 add group name for telephone A (ABC Company).	Telephone A sends its group name (ABC Company) to telephone B.
Incoming, off-net. Two nodes connected over a public network, over an interface that supports name display.	LD 11 or LD 95: CPND-NAME for each telephone	Telephone A (private name A) calls B (private name B). Telephone A sends its private name (A) to telephone B.	Same as before, except in LD 95 add group name for telephone A (ABC Company).	Telephone A sends the name associated with its CLID entry, or group name (ABC Company), to telephone B.
On-net Two nodes over a private network.	The feature enhancement does not affect on-net calls. The same number is sent as before the CLID Name Enhancement.			

Figure 8
General setup: Three nodes, each with one telephone, A, B, and C.



Type of call	Previous configuration	Previous scenario	Change in configuration with CLID name enhancement	Change in outcome of scenario with CLID Name Enhancement
Tandem call on two private networks. Three nodes, each with one telephone, connected over private network links.	The feature enhancement does not affect calls going over a private network link. The same number is sent as before the CLID Name Enhancement.			
Tandem call on a private-public network. Three nodes and each node has one telephone. Nodes 1 and 2 are connected over a private network link and Node 2 and 3 are connected over a public network.	LD 11 or LD 95: CPND NAME for each of the three telephones.	Telephone A (private name A) calls telephone B over a private network. The call is placed tandem by telephone B over a public network to telephone C. Node 1 sends the name provisioned for the DN to node 2, which is tandem to node 3.	Same as before, except in LD 95 add group name for telephone A (ABC Company).	Node 1 sends the name associated with its CLID entry, or its group name (ABC Company), to node 2, which is tandem to Node 3.

Transferred call over private-public network (public protocol supports name display). Three nodes, each with one telephone. Node 1 is connected to Node 2 over a private network link, and node 2 is connected to node 3 over a public network. In this scenario, the public network protocol supports updating name and number after transfer and this feature is enabled.	LD 11 or LD 95: CPND-NAME for each telephone.	Telephone A (private name: A) calls telephone B over a private network, and a call transfer is completed by telephone B over a public network to telephone C. The transferring node, telephone B, sends the name of telephone C to telephone A and the name of telephone A to telephone C.	Same as before, except in LD 95 add group name for telephone B (ABC Company).	As the call is transferred from telephone B to C, telephone B sends the name associated with its CLID entry to telephone C. Once the transfer is complete from B to C, telephone A sends the name associated with its CLID entry to telephone C and telephone C sends its private name (C) to telephone A.
Transferred call over private-public network (public network does not support updating name display) Three nodes connected in a combination of a private network and a public network. Node 1 is connected to node 2 over a private network link and node 2 and 3 are connected over a public network.	LD 11 or LD 95: CPND-NAME for each telephone.	Telephone A calls telephone B over a private network and the call transfer is completed by telephone B over a public network to telephone C. The transferring node, telephone B sends the name of telephone C to telephone A and the name of telephone A to telephone C.	Same as before, except in LD 95 add group name for telephone B (ABC Company).	As the call is transferred from telephone B to C, telephone B sends its group name (ABC Company) to telephone C. Since in this scenario, the public network protocol does not support updating name and number after transfer, there is no change in the number sent after transfer is completed.

Redirection over a private-public network. Three nodes connected over a combination of private and public networks. Nodes 1 and 2 are connected over a private network link and node 2 is connected to node 3 over a public network.	The feature enhancement does not affect calls going over a private network link. The same number is sent as before the CLID Name Enhancement.			
Tandem call over a public-private network. Three nodes over a combination of private and public networks. Nodes 1 and 2 are connected over a public network and node 2 is connected to node 3 over a private network link.	LD 11 or LD 95: CPND-NAME for each telephone	Telephone A calls telephone B over a public network. The call is placed in tandem on a private network through telephone B to telephone C. Telephone A sends the name associated with its DN.	Same as before, except add a group name for telephone for C (XYZ Company) in LD 95.	Telephone C sends its group name (XYZ Company) to telephone A. Note that the call is from a public network to a private network, so group name is displayed only if name display is supported by the tandem node.
Transfer over a public-private network (public protocol supports name display update) Three nodes connected in a combination of a public network and a private network. Nodes 1 and 2 are connected over a public network	LD 11 or LD 95: CPND-NAME for each telephone.	Telephone A calls B over a public network and the call is transferred by telephone B over a private network to telephone C. Telephone A sends its private name to telephone C.	Same as before, except in LD 95, add group name for telephone A (ABC Company) and a group name for telephone C (XYZ Company).	Telephone A calls B over a public network and the call is transferred by telephone B over a private network to telephone C. With the enhancement, as telephone B transfers the call to telephone C, it sends its private name to C.

and Nodes 2 and 3 over a private network link. For this scenario, the public network protocol supports updating name and number after transfer.				When the transfer is complete, telephone A sends its private name to telephone C.
Redirection over public-private network. Three nodes, 1 (CO), 2, and 3 with three telephones, A, B, and C. Nodes 1 and 2 are connected over a public network and Nodes 2 and 3 over a private network link.	The feature enhancement does not affect calls going over a private network link. The same number is sent as before the CLID Name Enhancement.			

Operating Parameters

If the DN for which the group name has to be sent does not have an associated CLID entry configured, the group name configured for the default entry, (for example, CLID entry zero is sent).

If a valid terminating terminal number is not available, then the group name configured for the default entry, (for example CLID entry zero, is sent).

If a call from the public network arrives with a truncated digit interface, the TON is usually mapped to unknown or the call type changes to abbreviated. Therefore, after an incoming call to the CS 1000 uses this truncated number, no group name can be sent back to the PSTN.

Privacy and security

Conditions under which a name is transported

The following table lists the only ISDN protocols over which CS 1000 supports name transport. The Remote Capabilities (RCAP) value is to be configured as ND2. If RCAP is already configured as ND1, ND1 has to be removed from a Meridian Customer Defined Network (MCDN) (SL1) interface to allow RCAP modification to ND2.

Table 14
The RCAP value of the interface

INTERFACE	RCAP
SL1	ND1/ND2/ND3
QSIG	ND1/NDO
EURO	UUSI
NI2	NDS
SL100,D100	ND2

Conditions under which a name is displayed

The presentation indicators for a telephone are determined by the Class of Service (CLS) value of the user. This CLS can be any of the following values:

- NAMA/NAMD
- Calling Name Display Allowed (CNDA) or Calling Name Display Denied (CNDD)
- Diverting Name Display Allowed (DNDA) or Diverting Name Display Denied (DNDD)

For these CLS values, it is the display that is affected. There is no change in the way the name is exchanged between two users.

The following are the indicators for the presentation of the name of a user:

- Connected Name Identification Presentation (CNIP): CNIP is a service offered to the called user and provides that user with the calling user's name. This service is permanent and based on the class of service NAMA defined (LD 10, LD 11) in the set originating the call.
- Connected Name Identification Presentation (CONP): CONP is a service offered to the calling user and provides that user with the name of the alerting, called, or connected user. This service is permanent and based on the class of service NAMA defined (LD 10, LD 11) on the set answering the call.
- Calling/Connected Name Identification Restriction (CNIR): CNIR is a service that prevents the served user's name from being presented to another user. This service is either activated for all calls (class of service

NAMD) or activated on a per-call basis for preventing presentation of the calling name information (class of service NAMA and Calling Party Privacy Flexible Feature Code dialed before initiating a call).

Error handling

Two new SCH error messages (SCH2204 and SCH2205) are introduced. Element Manager is updated to support the new error messages. The SCH error message is printed if the CLID entry input is invalid. A null input to the ENTR prompt results in a prompt for the next prompt.

Feature interactions

Call transfer

The changes in the display of a transferred call depend on whether the call goes over a public network or a private network link.

- If the call originates in a private network link, the private name of the caller is sent to the other end. The private or group name of the connected user is sent, depending on whether the call lands on a public or a private network link.
- If the call originates in a public network, the group name of the caller is sent to the other end. The private or group name of the connected user is sent, depending on whether the call lands on a public or a private network link.

ISDN CLID Enhancement

The CLID Name Enhancement feature interacts with the ISDN CLID Enhancement. The ISDN CLID Enhancement feature is useful in situations where it is important to see the originator's number and name at the terminating telephone instead of that of the transferring party in a call transferred across an SL1 trunk interface.

If the ISDN CLID feature is turned on, when the transferring party initiates the call transfer across the network (SL1 interface), the CLID information of the original caller is sent to the other node in the setup message. The original caller's name displayed after the transferring party initiates the call transfer is dependent on the name sent across the network where the call originated.

If the ISDN CLID Enhancement feature is turned on and if the call originated within the same node, the private name of the originating party is displayed (if configured). If the call originated across a public network, then the group name is displayed (if configured).

Call forward all calls, hunt, no answer, and busy

Using call forward all calls, call forward no answer, call forward busy, or hunt allows callers to manually forward, or forward on a no answer, or forward on busy, to any other station on the ISDN network. The receiving location is provided with the dialed number, the calling number, and if CPND is provisioned, the name of the caller and the reason for redirection.

- Call forward all calls: The originating and the terminating ends can have a change in their displays depending on the networks. The call forwarding node does not have any display involved. The originating node and the connected node send their public or private names depending on whether it is an off-net call or on-net call.
- Call forward no answer, call forward busy, and Hunt: The originating and the terminating ends can have a change in their name, depending on the networks. If the call is off-net, the call forwarding node has the group name of the originating node while that telephone is ringing. If the call is an on-net call, the private name is sent.

Connected number

If there is call modification such as call transfer, a connected number and its name are sent in the ISDN Notify/Connect message for the MCDN peer-to-peer networks or in the facility message for UIPE networks. The connected name is obtained from the CPND name that is stored along with the source key for the telephone. If possible, the CLID Name Enhancement feature uses the group name stored in the CLID entry associated with the active DN key if the call is over a public network. If the active DN does not have any entry number associated, the group name to be displayed is taken from CLID entry 0, the default CLID entry, if group name is configured.

Calling party name display

Currently, Calling Party Name is constructed using the DN of the active DN key. With this feature, the construction of the Calling Party Name depends on the network on which the call originates. If the call is over a private network link or if there is no other name associated with the DN, the CPND name associated with the source key of the DN is used for name display. Alternately, if the call is on a public network and has a CLID entry associated with the DN, the group name is taken from the associated CLID entry of that DN. If the active DN does not have entry number associated, the name configured for the default CLID entry, if configured, is sent.

Network call redirection

The originating and terminating parties names are interchanged. If a group name is configured, that group name is sent. The CLID Name Enhancement feature works for network redirection only when NCRD is turned on.

Numbering plan interactions

If the call redirected within a private network link has the TON and the Numbering Plan of the originally called number is public, group name is displayed.

Trunks involved

The CLID Name Enhancement feature has functionality for PRI and PRI2 trunk types. The changes are not applicable for DTI or DTI2.

Feature packaging

The CLID Name Enhancement feature requires the following packaging:

- Calling Party Name Display (CPND) package 95
- Integrated Services Digital Network (ISDN) package 145
- Integrated Services Digital Network Supplementary services (ISDNS) package 161
- Call Identification (CALL ID) package 247
- Digit Display (DIGDSP) package 19

Feature implementation

Implementation using overlays

CS 1000 Release 5.0 introduces the new prompt ENTR. The new prompt ENTR is added in LD 95 to allow group name configuration for an entry number to a CLID data block defined in LD 15. The overlay confirms that the ENTR value entered is valid, and a new SCH error message is printed whenever the CLID entry value is invalid.

The ENTR prompt takes a numeric value as input. If the CLID entry is configured for the customer in the Customer Data Block (CDB), the group name is taken as input for that entry. If a NULL input is entered for the ENTR prompt, the overlay prompt moves to the next prompt. This group name is associated to the DN, based on the CLID entry configured for the DN, while the key name or the key function and the DN are configured as the telephones are configured. If a valid ENTR number is entered, the overlay prompts for the group name associated with this CLID entry block, the expected length, and the display format. Following the entry of these fields, the overlay re-prompts ENTR. This continues until “NULL” is entered.

Task summary list

The following is a summary of the tasks in this section:

- LD 95—Configure CPND name
- LD 95—Configure group name

- LD 11—Configure group name

Table 15
LD 95—Configure CPND name

Prompt	Response	Description
REQ	NEW, CHG	Req = NEW or CHG to change an existing Customer Data Block)
TYPE	NAME	Type = Name of data block
CUST	xx	Customer number associated with this telephone
...		
ENTR	x	Entry number
NAME	xxx	Group name in calling party name display
- DISPLAY_FMT	aaaa.bbbb	Display format for calling party name display
ENTR		Entry number

Two new warning messages are introduced to indicate that the:

- the input CLID entry number is not configured for the customer in CDB
- the input value entered is greater than the default maximum-allowed CLID entry

The print routine for LD 95 is modified to print the new prompt value of Name in the Customer Data Block (CDB).

This feature enhancement retains all the conditions necessary for the transport of name to the next user and also for the display of the received name of any user. A protected variable CLID_NAMEP is added in the CDB CLID entry blocks in the unprotected data store. The feature enhancement is applicable for all digital telephones and analog telephones that have name display.

The function of the CLID Name Enhancement during a call transfer depends on whether a call takes place over a public network or a private network link.

This feature enhancement has interactions with another CLID feature enhancement introduced by CS 1000 Release 5.0, called ISDN CLID Enhancement. The ISDN CLID Enhancement comes into play in cases when it is important that a terminating telephone display the name and number of an originating telephone during a call transfer, instead of the name and number of the telephone performing the transfer.

The common name in the NAME prompt in LD 95 must be configured at both the nodes. This is configurable as a string of characters.

The CLID entry for which the group name is configured is associated to the DN while configuring the set in LD 11 or in LD 10.

Table 16
LD 11 - Configure group name

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW	Configure a new telephone
TYPE	xxx	Type of telephone
CUST	xx	Customer number
...		
...		
KEY	x aaa yyy (cccc or D)	xx = Key number aaa = Key name or function (SCR/MCR/PVN/PVR/SCN) yyyy = DN cccc = CLID table entry of (0)-N, where N = the value entered at the SIZE prompt in LD 15 minus 1. D = the character D. After the character D is entered, the system searches the DN keys from key 0 and up to find a DN key with a CLID table entry. The CLID associated with the found DN key is then used.
...		

Implementation using Element Manager

A new prompt ENTR is added in LD 95 to allow group name configuration for each entry number of a CLID data block, defined in LD 15.

Use the following procedure to configure Group CLID Name for a new customer.

Configuring Group CLID Name

Step	Action
1	Log on to Element Manager using a valid user account.
2	Go to the **Customers** page.
3	Click **Add...** to load the **Basic Configuration** page.

4 Enter valid values for parameters in the **Basic Configuration** page and click **SAVE**.

The Edit page displays.

5 Click the **ISDN and Electronic Switched Network (ESN)** link on the Edit page.

The **ISDN and ESN** page displays.

6 Click the **Calling Line Identification Entries** link.

7 Click **Add...** in the **Calling Line Identification Entries** table to load the **New Calling Line Identification** page.

If the CPND is not already configured, a popup appears stating, "Group Names require CPND to be configured. Click OK to configure CPND for the customer."

New input fields appear in the New Calling Line Identification page (the Roman characters block and the Katakana characters block, each containing group name, Expected length, and Display format fields).

8 Enter valid values in the fields on the **New Calling Line Identification** page and click **Save**.

Note: The Expected length field value is context-sensitive and cannot exceed the maximum-length (MXLN) value configured for the Customers > Call Party Name Display section. The value entered for group name cannot exceed the value specified in the Expected length field.

Calling Line Identification entries are displayed with the new values updated. The new values are updated to the specified customer data block and CPND block.

—End—

Use the following procedure to create a Group CLID Name for an existing CLID entry.

Configuring Group CLID Name for an existing CLID entry

Step	Action
1	Log on to Element Manager with a valid user account.
2	Go to the **Customers** page.

3 Click the listed customer number in the table that has the CLID entry already configured to display the **Edit** page.

4 Click the **ISDN and ESN** link on the Edit page to load the ISDN and ESN page.

5 Click the **Calling Line Identification Entries** link.

6 Click any of the listed CLID entries from the **Calling Line Identification Entries** table to load the **Edit Calling Line Identification (##)** page.

New input fields for CPND Language (the Roman characters block and the Katakana characters block, each containing Group name, Expected length, and Display format fields), are displayed on the Edit Calling Line Identification (##) page. The Expected length field value is context-sensitive and cannot exceed the maximum-length (MXLN) value configured for the Customers > Call Party Name Display section. The value entered for group name field cannot exceed the value specified in the Expected length field.

7 Enter valid values for the fields and click **Save**.

Calling Line Identification Entries are displayed with the new values updated. The new values are updated to the specified customer data block and CPND block.

—End—

Use the following procedure to edit an existing CLID group name.

Editing an existing CLID group name

Step	Action
1	Log on to Element Manager with a valid user account.
2	Go to the **Customers** page.
3	Click the listed customer number in the table that has the CLID entry already configured to display the **Edit** page.
4	Click the **ISDN and ESN** link on the **Edit** page to load the ISDN and ESN page.
5	Click the **Calling Line Identification Entries** link.
6	Click any of the listed CLID entries from the **Calling Line Identification** Entries table to load the**Edit Calling Line Identification (##)** page.

Under the CPND Language section, the Expected length field must be non-editable for the existing group name.

7 Edit the group name or the display format field, or both, and click **Save**.

Calling Line Identification Entries are displayed with the new values updated. The new values are updated to the specified customer data block and CPND block.

—End—

Use the following procedure to configure the ISDN and ESN page layout.

Configuring the ISDN and ESN page layout

Step	Action
1	Log on to Element Manager with a valid user account.
2	Go to the **Customers** page.
3	Click the listed customer number in the table to display the **Edit** page.
4	Click the **ISDN and ESN** link on the **Edit** page to load the **ISDN and ESN** page.

—End—

Use the following procedure to configure the Calling Line Identification Entries page layout.

Configuring the Calling Line Identification Entries page layout

Step	Action
1	Log on to Element Manager with a valid user account.
2	Go to the **Customers** page.
3	Click the listed customer number in the table to display the **Edit** page.
4	Click the **ISDN and ESN** link on the Edit page to load the **ISDN and ESN** page.
5	Click the **Calling Line Identification Entries** link to load the **ISDN and ESN (Calling Line Identification Entries)** page.

—End—

Use the following procedure to configure the New Calling Line Identification page layout.

Configuring the New Calling Line Identification page layout

Step	Action
1	Log on to Element Manager with a valid user account.
2	Go to the **Customers** page.
3	Click the listed customer number in the table to display the **Edit** page.
4	Click the **ISDN and ESN** link on the **Edit** page to load the **ISDN and ESN** page.
5	Click the **Calling Line Identification Entries** link to load the **ISDN and ESN (Calling Line Identification Entries)** page.
6	Click **Add...** in the **Calling Line Identification Entries** table to load the**New Calling Line Identification (##)** page.

—End—

Use the following procedure to configure the Edit Calling Line Identification page layout.

Configuring the Edit Calling Line Identification page layout

Step	Action
1	Log on to Element Manager with a valid user account.
2	Go to the **Customers** page.
3	Click the listed customer number in the table to display the **Edit** page.
4	Click the **ISDN and ESN** link on the Edit page to load the ISDN and ESN page.
5	Click the **Calling Line Identification Entries** link to load the ISDN and ESN (Calling Line Identification Entries) page.

6 Click any of the listed CLID entries from the **Calling Line Identification Entries** table to load the **Edit Calling Line Identification (##)** page.

—End—

ISDN CLID Enhancement

Feature description

Integrated Services Digital Network (ISDN) Calling Line Identification (CLID) Enhancement is an enhancement to name and number delivery on call transfers and conference calls.

Before the enhancement, a telephone receiving a transferred call during a call transfer was sent the name and number of the telephone transferring the call. With this feature enhancement, a telephone receiving a transferred call can be sent the name and number of the telephone transferring the call, or the name and number of the originating telephone.

This enhancement is vital in emergency situations when it is critical to see the name and number of the originating telephone on the terminating telephone, even before the transfer is complete. If a fire department transfers an emergency call to an ambulance service, for example, it is important for the ambulance service to see the name and number of the originating telephone of the person with the emergency, not that of the fire department.

This feature enhancement provides identical options within the setup of a conference call. The telephone added to a conference call can be sent the name and number of the telephone that added the telephone to the conference call, or the name and number of the originating telephone.

The ISDN CLID Enhancement applies to all users who use telephone display and voice mail. The enhancement applies to all digital telephones as well as analog (500/2500-type) telephones that support name display. This feature is restricted to MCDN/IP Peer tunneled networks and is only applicable to SL1 trunks and ISDN trunks. The feature enhancement is not packaged.

This feature enhancement is supported only for calls going on MCDN/H.323/SIP networks.

In H.323 networks, name display is provided when the information is available in either direction, that is, H.323 to ISDN, or ISDN to H.323.

Feature restrictions

ISDN CLID Enhancement is limited to calls transferred or conferenced locally or across the MCDN network with SL1 interface.

This feature handles only Call Transfer and Conference scenarios.

ISDN CLID Enhancement does not work with access code.

If the feature is turned on, in some scenarios, the terminating telephone receives a voice mail identified as coming from the originating telephone instead of the transferring telephone. This occurs, for example, after an incoming emergency call is transferred to a different node redirected at the terminating telephone to a local or remote CallPilot. With this type of call, the information of the telephone originating the call is sent to the terminating telephone in the setup message.

The ISDN CLID Enhancement is designed for emergency calls, where it is critical for the terminating telephone to see the details of the originator, even before the transferring party completes the transfer operation. In a true emergency situation, for example, where a call is transferred to a fire department or police department, and the feature is turned on, it is more likely that the call is intercepted by a device capable of Interactive Voice Response (IVR), such as CallPilot than, by voice mail. A device with IVR can prompt a caller to choose a number for a specific service, for example, the caller can choose 1 for fire, 2 for police, and 3 for ambulance.

CallPilot can also be an automated attendant or a company can use a live switch board hired for handling such scenarios. There is little to no possibility that an emergency caller leave a voice mail on the terminating telephone.

This feature must not be used where the IP connection is used to place calls to the Public Switched Telephone Network (PSTN). For example, in Norway, the H.323 interface is used to connect to the public network. This public network can screen every call to ensure that the CLID belongs to the IP address placing the call. This means, if the feature is turned on and a call comes from the PSTN and the user at the CS 1000 transfers the call back to the PSTN, the PSTN rejects the call. The setup must contain the public network number of the person transferring a call or the call is rejected. In places where the H.323 link is used to connect to the public network, either two separate and discrete signaling servers or Dedicated Transport Channels (DCHs) are required, one for the PSTN and one for the private network. Otherwise, the ISDN CLID Enhancement cannot be used.

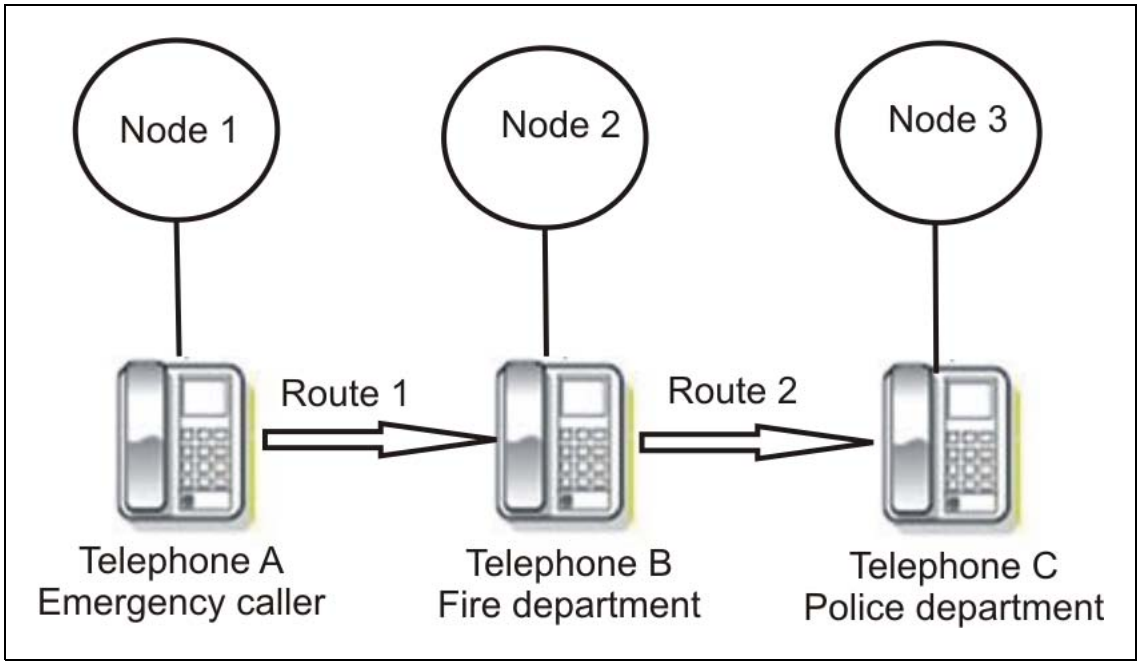
Over IP, the new field in the Calling Party Number Information Element (IE) can be lost. It is always lost for Session Initiation Protocol (SIP) because the IE has its data mapped into native mode SIP and then IE is discarded. For H.323, if the number is changed by a CS 2000 or other PSTN type

gatekeeper, the original IE is discarded, and the substituted IE is used. The data in the tunneled nonstandard data is ignored. For this feature to work, all nodes must be Meridian 1. This feature does not work with third-party Private Branch Exchange (PBX).

The following section describes sample scenarios and the effect of the ISDN CLID Enhancement on transferred calls. This feature enhancement operates in the same manner during conference calls.

Sample scenarios

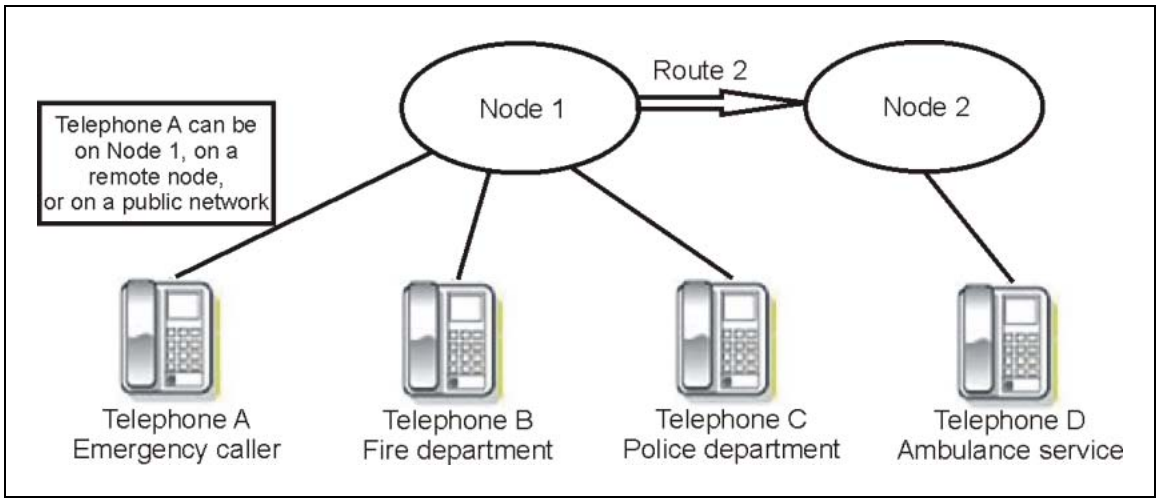
Figure 9
Sample scenario——three nodes, three telephones



Type of call	General setup	Scenario before the ISDN CLID Enhancement	Change in outcome of scenario with ISDN CLID Enhancement turned on
Incoming call (see figure: Sample scenario——three nodes, three telephones	There are three nodes, node 1, node 2, and node 3, and three telephones, A, B, and C. Telephone A is on node 1, is on a remote node, or is on a public network. Telephone B is on Node 2 and telephone C is on node	Telephone B receives an incoming call from telephone A. Telephone B initiates a call transfer to telephone C. Telephone C displays the name and number of telephone B while ringing. After the	DORG is set to YES on the outgoing SL1 route 2 from node 2 to node 3. LD 95 ECSL = CSLT on node 3. In a local transfer, where the transferring telephone and transferred to telephone are on

	3. Telephone C has display capability. Node 2 and 3 are connected by an MCDN network.	transfer is complete, telephone C displays telephone A as the caller.	the same node, the DANI prompt on the terminating telephone makes the decision of displaying either the CLID of the originating telephone or the CLID of the terminating telephone. With the ISDN CLID Enhancement, the ECSL prompt in LD 95 is set to any string 4 characters in length, in this case, CSLT. This indicates to telephone C that this particular call is a special case and the name and number represents the originating party and not the transferring party.

Figure 10
Sample scenario——two nodes, four telephones



Type of call	General setup	Scenario before the ISDN CLID Enhancement	Change in outcome of scenario with ISDN CLID Enhancement turned on
Incoming call transferred by attendant (See figure: Sample scenario——two nodes, four telephones)	There are two nodes, node 1 and node 2, and four telephones, A, B, C, and D. Telephone A can be on Node 1, on a remote node, or on a public network. Telephones B and C are on Node 1. Telephone D, which supports display, is on Node 2. Nodes 1 and 2 are connected by the MCDN network and route 2 must use SL1/IP Peer trunks.	In a local transfer, telephone B receives a call from telephone A. Telephone B initiates a call transfer to telephone C. Telephone C rings and displays telephone B as the caller. In a network transfer, telephone B receives a call from telephone A. Telephone B initiates a call transfer to telephone C. Telephone C rings and displays the name and number of telephone B. Telephone C initiates a call transfer to telephone D across the trunk. Telephone D rings and displays the name and number of telephone C as the caller.	DORG is set to YES on the outgoing route from node 1 to node 2. Telephone C has DANI set to yes and LD 95 ECSL = CSLT. In a local transfer, telephone B receives the call from telephone A. Telephone B initiates a transfer to telephone C. Telephone C rings and displays the name and number of telephone A as the calling number. In a network transfer, telephone B receives a call from telephone A. Telephone B initiates a call transfer to telephone C. Telephone C rings and displays the name and number of telephone A as the caller. Telephone C initiates a call transfer to telephone D across the trunk. Telephone D rings and displays the name and number of telephone A.

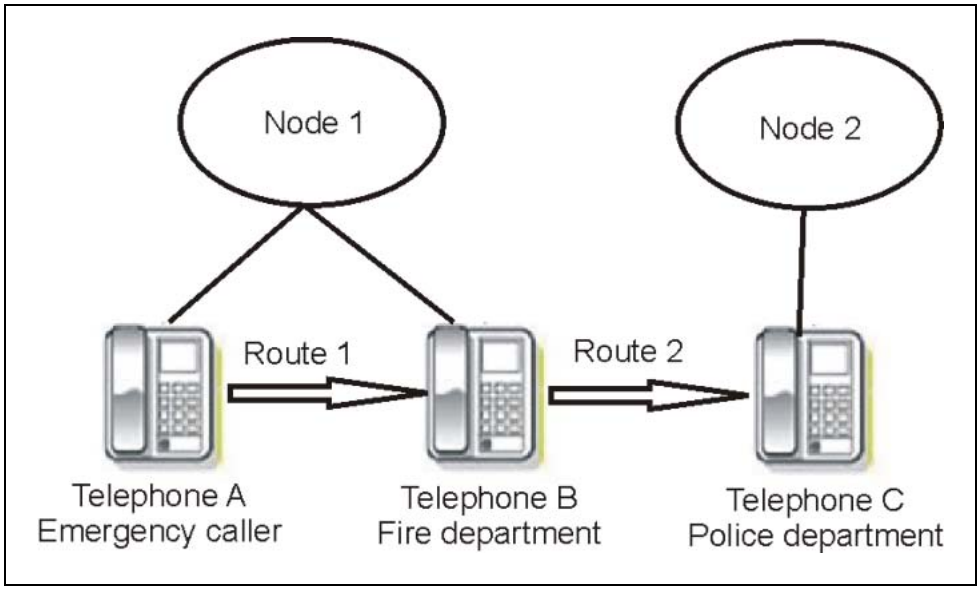
Incoming call transferred by attendant (see figure: Sample scenario——two nodes, four telephones)	There are two nodes, node 1 and node 2, and four telephones, A, B, C, and D. Telephone A can be on Node 1, on a remote node, or on a public network. Telephones B and C are on Node 1. Telephone D, which supports display, is on Node 2. Nodes 1 and 2 are connected by the MCDN network and route 2 must use SL1/IP Peer trunks.	In a local transfer, telephone B (the attendant) receives a call from telephone A. Telephone B (the attendant) initiates a call transfer to telephone C. Telephone C rings and displays Telephone B (the attendant) as the caller. In a network transfer, telephone B (the attendant) receives a call from telephone A. Telephone B (the attendant) initiates a call transfer to telephone C. Telephone C rings and displays the name and number of telephone B. Telephone C initiates a call transfer to telephone D across the trunk. Telephone D rings and displays the name and number of telephone B as the caller.	DORG is set to YES on the outgoing route from node 1 to node 2. Telephone C has DANI set to yes and LD 95 ECSL = CSLT. In a local transfer, telephone B (the attendant) receives the call from telephone A. Telephone B (the attendant) initiates a transfer to telephone C. Telephone C rings and displays the name and number of telephone A as the calling number. In a network transfer, telephone B (the attendant) receives a call from telephone A. Telephone B (the attendant) initiates a call transfer to telephone C. Telephone C rings and displays the name and number of telephone A as the caller. Telephone C initiates a call transfer to telephone D across the trunk. Telephone D rings and displays the name and number of telephone A.
Incoming call transferred by an ACD agent (See figure: Sample scenario——two nodes, four telephones)	There are two nodes, node 1 and node 2, and four telephones, A, B, C, and D. Telephone A can be on Node 1, on a remote node, or on a public network. Telephone B (ACD agent) and telephone C are on Node 1. Telephone D, which supports display, is on Node 2. Nodes 1 and	In a local transfer, telephone B (the ACD agent) receives a call from telephone A. Telephone B (the ACD agent) initiates a call transfer to telephone C. Telephone C rings and displays Telephone B (the ACD agent) as the caller. In a network transfer, telephone B (the ACD agent) receives a call	DORG is set to YES on the outgoing route 2 from node 1 to node 2. Telephone C has DANI set to yes and LD 95 ECSL = CSLT. In a local transfer, telephone B (the ACD agent) receives the call from telephone A. Telephone B (the ACD agent) initiates a transfer to telephone C.

	2 are connected by the MCDN network and route 2 must use SL1/IP Peer trunks.	from telephone A. Telephone B (the ACD agent) initiates a call transfer to telephone C. Telephone C rings and displays the name and number of telephone B. Telephone C initiates a call transfer to telephone D across the trunk. Telephone D rings and displays the name and number of telephone B (the ACD agent) as the caller.	Telephone C rings and displays the name and number of telephone A as the calling number. In a network transfer, telephone B (the ACD agentt) receives a call from telephone A. Telephone B (the ACD agent) initiates a call transfer to telephone C. Telephone C rings and displays the name and number of telephone A as the caller. Telephone C initiates a call transfer to telephone D across the trunk. Telephone D rings and displays the name and number of telephone A.
Incoming call transferred by CallPilot	There are two nodes, node 1 and node 2, and four telephones. Telephone A can be on Node 1, on a remote node, or on a public network. Node 1 has Meridian Mail/CallPilot VSDN (telephone B) and telephone C. Telephone D is on node 2 supports display. Nodes 1 and 2 are connected by the MCDN network and route 2 must use SL1/IP Peer trunks.	In a local transfer, Meridian Mail/CallPilot VSDN on node 1 (telephone B) receives a call from telephone A. Meridian Mail/CallPilot VSDN initiates a call transfer to telephone C. Telephone C rings and displays Meridian Mail/CallPilot VSDN as the caller. In a network transfer, Meridian Mail/CallPilot VSDN receives a call from telephone A. Meridian Mail/CallPilot VSDN initiates a call transfer to telephone D on node 2. Telephone D rings and displays MNAIL/CallPilot VSDN as the caller.	DORG is set to YES on the outgoing route 2 from node 1 to node 2. Telephone C has DANI set to yes and LD 95 ECSL = CSLT. In a local transfer, Meridian Mail/CallPilot VSDN receives the call from telephone A. Meridian Mail/CallPilot VSDN initiates a transfer to telephone C. Telephone C rings and displays the name and number of telephone A as the calling number. In a network transfer, Meridian Mail/CallPilot VSDN receives a call from telephone A. Meridian Mail/CallPilot VSDN nitiates a call transfer to telephone C. Telephone C rings and displays the

			name and number of telephone A as the caller. Telephone C initiates a call transfer to telephone D across the trunk. Telephone D rings and displays the name and number of telephone A.
Incoming call transferred by CallPilot to SCCS (See figure: Sample scenario——two nodes, four telephones)	There are two nodes, node 1 and node 2, and four telephones. Telephone A can be on Node 1, on a remote node, or on a public network. Node 1 also has Meridian Mail/CallPilot VSDN and telephone C. Telephone D, the telephone of a local SCCS agent, which supports display, is on Node 2. Nodes 1 and 2 are connected by the MCDN network and route 2 must use SL1/IP Peer trunks.	In a local transfer, Meridian Mail/CallPilot VSDN receives a call from telephone A. Meridian Mail/CallPilot VSDN initiates a call transfer to telephone C. Telephone C rings and displays Meridian Mail/CallPilot VSDN as the caller. In a network transfer, Meridian Mail/CallPilot VSDN receives a call from telephone A. Meridian Mail/CallPilot VSDN initiates a call transfer to telephone C. Telephone C rings and displays the name and number of telephone B. Telephone C initiates a call transfer to telephone D (the SCCS agent) across the trunk. Telephone D (the SCCS agent) rings and displays Meridian Mail/CallPilot VSDN as the caller.	DORG is set to YES on the outgoing route 2 from node 1 to node 2. Telephone C has DANI set to yes and LD 95 ECSL = CSLT. In a local transfer, Meridian Mail/CallPilot VSDN receives the call from telephone A. Meridian Mail/ CallPilot VSDN initiates a transfer to C. Telephone C rings and displays the name and number of telephone A as the calling number. In a network transfer, Meridian Mail/CallPilot VSDN receives a call from telephone A. Meridian Mail/ CallPilot VSDN initiates a call transfer to C. Telephone C rings and displays the name and number of telephone A as the caller. Telephone C initiates a call transfer to D (the SCCS agent) across the trunk. Telephone D (the SCCS agent) rings and displays the name and number of telephone A.

IP-related scenario (See figure: Sample scenario——two nodes, four telephones)	There are two nodes, node 1 and node 2, and four telephones, A, B, C, and D. Telephone A can be on Node 1, on a remote node, or on a public network. Telephone B and telephone C are on node 1. Telephone D, which supports display, is on node 2. Nodes 1 and 2 are connected by an IP Peer network and route 2 must use SL1/IP Peer trunks.	In a local transfer, telephone B receives an incoming call from telephone A. Telephone B initiates a call transfer to telephone C, and C rings and displays telephone B as the caller. In a network transfer, telephone B receives an incoming call from telephone A. Telephone B initiates a call transfer to telephone D across the trunk. Telephone D rings and displays telephone B as the caller.	DORG is set to YES on the outgoing route 2 from node 1 to node 2. Telephone C has DANI set to yes and LD 95 ECSL = CSLT. In a local transfer, telephone B receives a call from A. Telephone B initiates a transfer to C. Telephone C rings and displays the name and number of telephone A as the calling number. In a network transfer, telephone B receives a call from A. Telephone B initiates a call transfer to C. Telephone C rings and displays the name and number of telephone A as the caller. Telephone C initiates a call transfer to D across the trunk. Telephone D rings and displays the name and number of telephone A.

Figure 11
Sample scenario——two nodes, three telephones



Type of call	General setup	Scenario before the ISDN CLID Enhancement	Change in outcome of scenario with ISDN CLID Enhancement turned on
Incoming call transferred to a different node redirected to local Meridian Mail/ CallPilot. (See figure: Sample scenario——two nodes, three telephones)	There are two nodes, node 1 and node 2, and three telephones, A, B, and C. Telephone A can be on Node 1, on a remote node, or on a public network. Telephone B is on node 1. Node 2 has telephone C. Telephone C supports display and has CFNA configured to local Meridian Mail/CallPilot. Nodes 1 and 2 are connected by the MCDN network and route 2 must use SL1/IP Peer trunks.	Telephone B receives an incoming call from telephone A. Telephone B initiates a transfer to telephone C, telephone C rings and displays telephone B as the caller. Telephone C has CFNA configured to local Meridian Mail/CallPilot. The call reaches the voice mail of telephone C and leaves a voice message from telephone B.	DORG is set to YES on the outgoing SL1 route 2 from node 1 to node 2. LD 95 ECSL = CSLT on node 3. Telephone B receives an incoming call from telephone A. Telephone B initiates a transfer to telephone C, telephone C rings and displays telephone A as the caller. Telephone C has CFNA configured to local Meridian Mail/CallPilot. The call reaches the voice mail of telephone

			C and leaves a voice message from telephone A.
Incoming call transferred across to a different node redirected to remote CallPilot. (See figure: Sample scenario——two nodes, three telephones)	There are two nodes, node 1 and node 2, with three telephones, A, B, and C. Telephone B is on node 1, a different node or on a public network. Telephone A is on node 1 and telephone B, which supports call display, is on node 2. Telephone B has CFNA configured to remote Meridian Mail/CallPilot. Node 1 and node 2 are connected by the MCDN network, and route 2 must use SL1/IP Peer trunks.	Telephone B receives an incoming call from telephone A. Telephone B initiates transfer to telephone C, telephone C rings and displays telephone B as the caller. Telephone C has CFNA configured to local Meridian Mail/CallPilot. The call reaches the voice mail of telephone C and leaves a voice message from telephone B.	DORG is set to YES on the outgoing route 2 from node 1 to node 2. LD 95 ECSL = CSLT. Telephone B receives a call from telephone A and initiates a call transfer to telephone C,. Telephone C rings and displays telephone A as the caller. Telephone C has CFNA configured to local Meridian Mail/CallPilot. The call reaches the voice mail of telephone C and telephone A leaves a voice message from telephone A.

Feature interactions

CDR: Abandon record (B)

This feature alters the details printed in the Abandon (B) record. In Call Transfer and Conference, the CLID of the originating telephone is sent in the SETUP message. The secondary call is considered abandoned when the terminating telephone rings. In this case, the Abandon record (B) has ORIGID as the originating telephone CLID and not the transferring telephone CLID. With the feature turned off, the Abandon record has the transferring telephone CLID in the ORIGID field of the CDR B record.

Display

In the Call Transfer or Conference scenario, the terminating telephone display shows the CLID of the originating telephone. This happens even while the telephone to which the call is transferred is ringing.

ACD

The construction of CLID in calls transferred by an Automatic Call Distribution (ACD) agent is same as when calls are transferred by any other telephone. The CLID of the originator is sent if the DORG prompt is set to Yes across the transfer route. In case of a local call transfer by an

ACD agent, the terminating telephone displays the CLID of the originating telephone and not the ACD DN. This specific scenario is already handled by ACD team.

Calling Party Name Display

Currently, Calling Party Name is constructed using the DN of the active DN key. For this feature, construction of the Calling Party Name is changed. The CLID information of the originator is sent to the terminating telephone instead of that of the transferring telephone, if the flexibility is enabled in the route. Otherwise, backward compatibility is maintained.

Administration from an Attendant Console

Administration of the CLID entry for a PBX or a Business Continuity System (BCS) telephone from an attendant is not supported.

Feature packaging

The ISDN CLID Enhancement feature requires the following packaging:

- Calling Party Name Display (CPND) package 95
- Integrated Services Digital Network (ISDN) package 145
- Integrated Services Digital Network Supplementary services (ISDNS) package 161
- Call Identification (CALL ID) package 247
- Digit Display (DIGDSP) package 19
- IP Peer H.323 Trunk (H323_VTRK) package 399
- SIP Gateway and Converged Desktop (SIP) package 406

Feature implementation

Implementation using overlays

The ISDN CLID Enhancement introduces one new prompts, Display Call Originator's Information (DORG).

In a local call transfer or conference, when the transferring telephone and the terminating telephone are on the same node, the Display Automatic Number Identification (DANI) prompt in LD 11 makes the decision on the terminating telephone to display either the CLID of the originating telephone or the CLID of the transferring telephone on the terminating telephone. Values of Yes or No can be chosen for DANI. If set to Yes, the CLID information of the originating telephone is displayed on the terminating telephone. If set to No, there is no change and the CLID information of the transferring telephone is displayed on the terminating telephone.

The new prompt DORG is introduced to the Route List Data Block in LD 86. DORG displays the CLID of the originating telephone at the terminating telephone in a call transfer or conference across the Meridian Customer Defined Network (MCDN). Values of Yes or No can be chosen for DORG. The default is No. If DORG is set to Yes, the name and number of the original caller is sent whenever there is a call transfer or conference on this route. The name and number appears on the terminating telephone even before the transfer or conference call is complete.

The prompt Emergency Consultation (ECSL) is available in the CPND data block in LD 95. ECSL can be set to any string of 4 characters in length. ECSL indicates in a call transfer that the call is a special case.

Task summary list

The following is a summary of the tasks in this section:

- LD 11—Configure DANI
- LD 86—Configure DORG
- LD 95—Configure ECSL

Table 17
LD 11 - Configure DANI

Prompt	Response	Description
REQ	NEW	Request = NEW
	CHG	Request = CHG
	PRT	Request = PRT
TYPE	2616	Type of data block = 2616
TN		Terminal Number
CUST		Customer number associated with this telephone
...		
DANI	(No) Yes	The CLID information of the originating telephone is displayed on the terminating telephone. If set to No, there is no change and the CLID information of the transferring telephone is displayed on the terminating telephone.

Table 18
Table 4: LD 86 - Configure DORG

Prompt	Response	Comment
REQ	NEW	Request = NEW
	CHG	Request = CHG

	PRT	Request = PRT
CUST		Customer number associated with this telephone
FEAT	RLB	Feature = RLB
ENTR		Entry
ROUT		Route number
...		
DORG	(No) Yes	The CLID information of the original caller is sent in the setup message. If it is set to No, there is no change in function of the feature and the CLID information of the transferring telephone is sent.

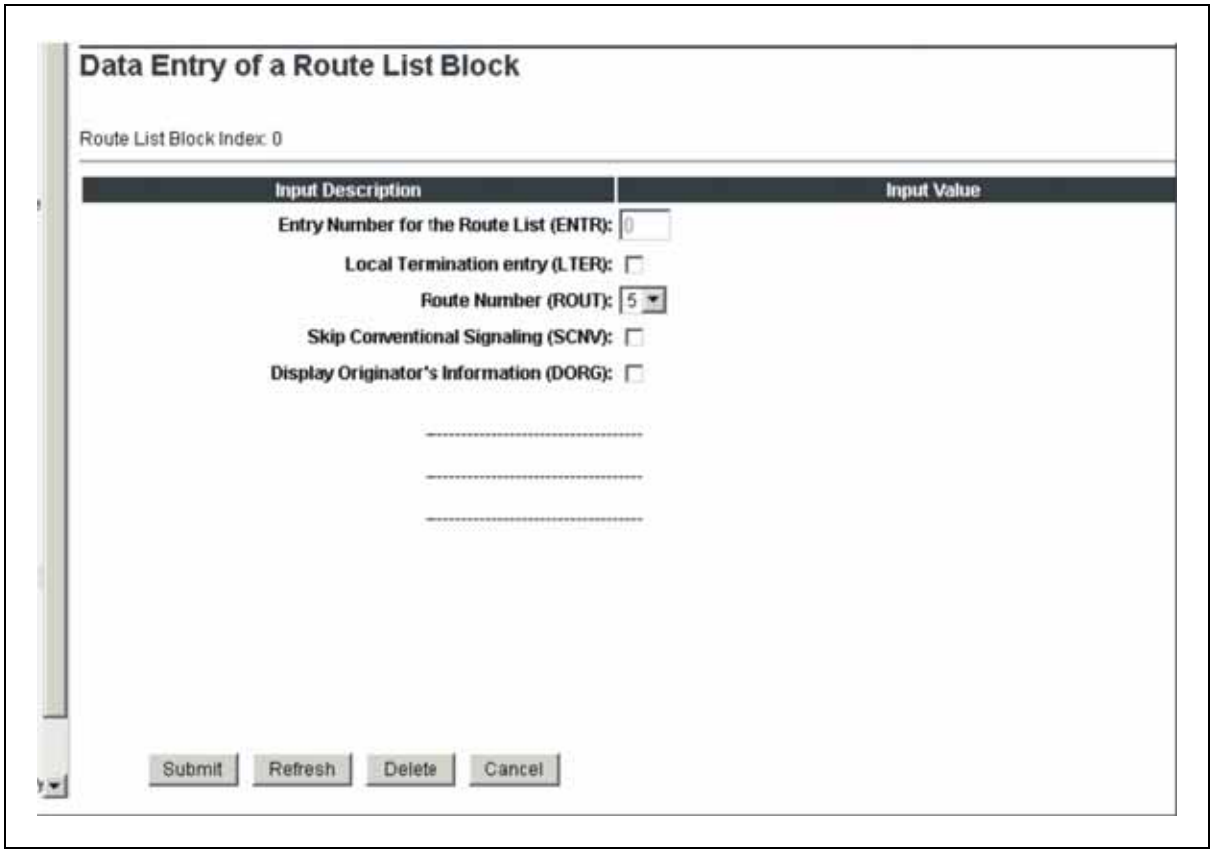
Table 19
LD 95 - Configure ECSL

Prompt	Response	Comment
REQ	CHG/NEW	Change an existing CPND block or configure a new CPND block
TYPE	CPND	CPND data block
CUST	2	Customer number
CNFG	alon	
MXLN	24	
STAL	yes	
DFLN	5	
DES	yes	
RESN	yes	Reason should be yes to configure ECSL; otherwise, ECSL prompt is not displayed.
CFWD		
CFNA		
HUNT		
PKUP		
XFEF		
AAA		
ECSL	CSLT	Emergency Consultation = Consultation Call This response indicates to the transferred to telephone that this is a special case. The response should not be greater than 4 characters.
NITC		

Implementation using Element Manager

The user network must be configured with TIE trunk. ISDN must be enabled for the TIE trunk. D-Channels and PRI or PRI2 loops should be configured for the server.

Figure 12
Element Manager - Data Entry of a Route List Block



Use the following procedure to configure DORG for the Route List Data Block.

Configuring DORG for the Route List Data Block

Step	Action
1	Log on to Element Manager with a valid user account
2	Navigate to **Dialing and Numbering Plans > Electronic Switched Network**
3	Navigate to **Customer XX > Network Control and Services > Route List Block.**
4	Add a new Route List Index. Enter the Route Number (ROUT) of a route for which a TIE trunk is configured.

5 Check the check box after the new prompt DORG is displayed.

6 Enter all the mandatory values and click **Submit**.

—End—

To edit DORG for a Route List Data Block, follow the next procedure.

Editing DORG for the Route List Block

Step	Action
1	Log on to Element Manager with a valid user account.
2	Navigate to **Dialing and Numbering Plans > Electronic Switched Network.**
3	Navigate to **Customer XX > Network Control and Services > Route List Block.**
4	Select the Route List Index to edit. Select **EDIT** next to the Route Number (ROUT) that is configured with the TIE trunk.
5	Check the check box after the new prompt DORG is displayed.
6	Enter all the mandatory values and click on **Submit**.

—End—

Bandwidth Management Support for Network Wide Virtual Office

Bandwidth Management Support for Network Wide Virtual Office (NWVO) allows the assignment of the same Virtual Private Network Identifier, VPNI, to all Call Servers in a network, such that the entire network can be identified by one VPNI number. It allows the assignment of the same Bandwidth Zone number to different Call Servers and to have an INTRAZONE policy between them. At the same time, this feature does not interfere with the existing functionality of the Bandwidth Management (BWM) feature, because previous bandwidth configuration rules are still supported. This feature extends the meaning of the Virtual Private Network Identifier (VPNI). In previous releases, VPNI was used to identify one customer system (Main Office (MO) switch + Branch Office (BO) switches connected to this MO switch). In CS 1000 Release 5.0, a VPNI number identifies the whole customer network that includes all MO and BO switches.

This feature introduces a new Current Zone field for the IP Phones to distinguish between the Bandwidth Zone number configured for the IP set and the current, real, zone number that is not configurable, but is changed dynamically by Virtual Office feature operation. The Current Zone field is used in the bandwidth calculation routines instead of the Configured Zone field to have correct bandwidth calculation in case of NWVO call scenarios. The customer can check the value of the Current Zone for IP Phones using LD 20, PRT command. This value is not configurable, no changes are made to LD 11.

For more information about the Bandwidth Management for Network Wide Virtual Office feature, see *Features and Services Fundamentals - Book 1 of 6 (NN43001-106-B1)*.

Network Music

Description

The Network Music feature allows a Communication Server (CS) 1000 system to be configured as a central audio source and supports Music on Hold (MOH) features without requiring a locally equipped music source. The central music source is accessed over the network by H.323/SIP virtual trunks.

Feature operation

The implementation consists of a central Audio Server to generate music. The Audio Server is accessible within the IP network by dialing a special DN. Music Trunks are installed on the remote nodes and connected back to back with an analog TIE trunk, which is auto-terminated to the primary DN of a Network Music Agent. The Network Music Agent forwards the call to the external DN of the Audio Server. When the music trunk is seized, it is connected to a call to the Audio Server through a H.323/SIP virtual trunk. Both broadcast and conference music are configured to allow multiple held parties to share the same music trunk.

Network Music Agent

The Network Music Agent:

- provides a local DN to access the Audio Server.
- can be configured using Personal Call Attendant (PCA).
  - — the DN assigned to the PCA is Attendant Directory Number (ATDN) of the Network Music TIE trunk.
  - — the target PCA DN contains the external DN of the Audio Server.
- can be configured using phantom TN.
  - — the DN assigned to the phantom TN is the ATDN of the Network Music TIE trunk.
  - — Default Call Forward (DCFW) of the phantom TN is the external DN of the Audio Server.

Music broadcast

To maximize resource efficiency, the music is broadcast so that multiple parties can share the same music trunk. A maximum of 64 listeners can be supported by one music trunk with broadcast music. Additionally, the conference music can be set up instead of broadcast by setting the Broadcast (BDCT) prompt of the music route to NO. A maximum of 29 simultaneous listeners can be supported by a single conference loop with one music trunk assigned. Communication Server 1000E only supports broadcast mode.

For more information on the Network Music feature, refer to *Features and Services Fundamentals - Book 4 of 6 (NN43001-106-B4)*.

System Management

In Communication Server 1000 Release 5.0, several components of the system management portfolio introduce enhancements that simplify system management tasks, improve the efficiency of multiple workflows and increase the scope and coverage of management applications. Specfically, CS 1000 Release 5.0 introduces enhancements to both Element Manager and Telephony Manager.

CS 1000 Release 5.0 introduces the Enterprise Common Manager Framework. The Enterprise Common Manager Framework is not specifically tied only to the CS 1000, but the CS 1000 is one of the early Call Server platforms to utilize this framework in the CS 1000 Release 5.0 software release.

Element Manager Enhancements

In Communication Server (CS) 1000 Release 5.0, Element Manager is enhanced to provide support for the Emergency Services Client Mobility feature.

When deployed on Linux operating system, Element Manager enables users to configure telephones for the Call Server.

Emergency Services

The Emergency Services Client Mobility feature allows users to manage the location of IP Phones, and to process emergency calls according to the caller's current data.

- The **Service Parameters** web page allows users to modify system-wide configuration settings
- The **Access Numbers and Routing** web page allows users to process Emergency Services information which are specific to each Customer.
- The **Response Locations** web page allows users to enable, disable or delete Emergency Response Locations (ERLs).
- The **Subnet Location Information** web pages allow users to modify subnet information.
- The **Dynamic Identification** web pages allow users to modify Dynamic Emergency Location information.

Phones

When clicking the **Phones** link in the Element Manager navigator for the very first time, Element Manager automatically performs a Database Update in the background. A message is displayed to the user: "Please wait for requested page to load while system properties are being updated..". The user can proceed to configure telephones after the update has been completed.

The following Phones functions can be performed using Element Manager:

- Search Phones

- Add Phones
- Retrieve Phones
- Delete Phones
- Swap Phones
- Move Phones
- Edit Phones
- Designation Strip
- Reports

Customers

In CS 1000 Release 5.0, Element Manager supports additional features used for the configuration of Customer data. These include:

- Application Module Link
- Call Detail Recording
- Call Party Name Display
- Call Redirection
- Centralized Attendant Service
- Controlled Class of Service
- Recorded Overflow Announcement
- Timers

Telephony Manager

Introduction

This chapter describes the changes in Telephony Manager (TM) for Release 3.1.

New and enhanced applications

Telephone Manager (Web Station) enhancements

- Support exists for operations for supported Meridian 1 and Communication Server (CS) 1000 releases and with global updates for all features.
- Any new telephones can be added. For a list of new telephones supported, refer to *Telephony Manager 3.1 System Administration (NN43050-601)*.
- Support for the prompts Terminal Number (NHTN) and Network UserID (NUID), in Media Gateway (MG) 1000B, CS 1000S, CS 1000M and CS1000E systems.
- New functionality is added to the Emergency Services for Client Mobility to support IP Phone mobility.
- Secure media exchanges between endpoints are allowed through a new class of service.
- All Phase II IP Phones and version II SoftPhones permit real-time recording and play of IP telephony sessions.
- CS 1000 Release 5.0 supports new features/key features and new operations on IP Phones.
- A new multi-language prompt is added to all IP Phones.
- A basic emergency service is available for Virtual Office Logged-Out (VOLO) telephones.
- New Terminal Number (TN) types are added to the Call Server and Line Terminal Proxy Server (TPS).
- Customer upgrades and new installations are supported by new hardware and software.

- The IP Line applicatioin is enhanced.
- New software and hardware extends the CS 1000M and CS 1000E.
- Two new daughterboards provide DSP resources for the connection of IP and TDM devices.
- TM reports are modified to display all telephones.
- TM client and TM server can be un-installed independent of each other.
- A new location report file is introduced for IP Phones in the TM inventory application.
- Correct bandwidth calculation available for those users using Virtual Office to login to their home IP Phones from different Call Servers within the network.

Web maintenance enhancements

- New hardware and software replaces the Small System Controller (SSC) when used as a gateway controller.
- Information is displayed in relation to Emergency Services Access (ESA) for the VOLO telephones.
- Two new daughterboards placed on the Media Gateway Controller (MGC) provide DSP resources for connecting IP and TDM devices.
- Thirteen new IP Phone types can be displayed in Web Maintenance.
- Information regarding the Virtual Office Logged Out (VOLO) telephones is displayed in the web maintenance application.
- New hardware provides updated configuration and maintenance commands.
- Diagnostic and fault reporting enhancements are added in Web maintenance and Alarm notification.
- A secondary location for registration of IP Phones in the event of a Signaling Server failure is provided by the new MC32S Media Card.

Alarm management enhancements

- A new category of Media Gateway Controller (MGC) type alarms can be used through the TM windows application.
- An administrator can view current alarms and control the filter and behavior of the system in the alarm interface.
- A patch for the Survivable Remote Gateway (SRG) 50 alarm subsystem provides survivability for IP Phones during a WAN failure.
- Simple Network Management Protocol (SNMP) provides support for the Linux operating system that runs Enterprise Common Management

framework (ECM), Network Routing Service (NRS), and Network Routing Service Manager (NRSM).

Alarm notification enhancements

- System alarms and messages are added to TM help.
- An error message is added to Call Server regarding media gateway configuration.

Traffic analysis enhancements

- Seven new fields are introduced to the QoS IP statistics report.
- Two new reports in traffic analysis display new traffic data.
- A new machine type, CS 1000E CP PM, is added as a new CPU option and is added under the "What-if" calculations in Traffic Analysis.
- A new customer report, DSP Peg Count, is generated only by the CS 1000M and CS 1000E systems.

Additional enhancements

- Support is provided for 911 calls to be redirected to another Meridian 1 over TIE trunks.
- DECT handsets display the unique Hex ID in site survey mode.

Global Address Book Synchronization

This feature is a Common Network Directory (CND) tool that allows a CallPilot network administrator to consolidate the local address books of all CallPilot Release 5.0 hosts in a network into a Global Address Book (GAB) whose entries are stored as subscribers in CND. In addition, this feature allows a CallPilot network administrator to keep a CND GAB entry up-to-date with respect to the CallPilot Release 5.0 local address book entry on which it originated.

For more information refer to *Common Network Directory 2.1 Administration* (NN43050-101).

Enterprise Common Manager

Enterprise Common Manager overview

The Enterprise Common Manager (ECM) provides users with an intuitive, common interface to manage and launch managed elements. ECM is a container that stores several system management elements in a single repository. Users need to sign in only once to access the elements. Users have access to all network system management elements in one framework. ECM eliminates the need for users to reauthenticate when they launch each system management application.

ECM provides framework-level security that simplifies security control for managed elements and system management applications. ECM manages secure access to Web applications and provides authentication and authorization with a single unified framework. ECM secures the delivery of essential identity and application information.

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

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

Enterprise Common Manager elements

The ECM framework is a resident Web-based management system used to configure and support the following managed elements:

- Network Routing Service
- Communication Server (CS) 1000 Release 5.0
- SIP Gateway
- Bookmark

Users access the framework through a Web browser such as Microsoft™ Explorer 6.02600 or later.

Key benefits and features

The ECM framework is a generic system management software application that provides the following key benefits and features:

- central launch point for management facilities that oversee multiple network elements to manage the entire network
- common UI look and feel across all supported management facilities
- generic infrastructure that includes the UI framework, security, backup and restore, and logging
- Web service interface where third-party developers can create applications to access ECM
- registry of the managed elements that launch the management applications
- security that provides Authentication, Authorization, and Auditing (AAA) for plug-in Web applications (elements) that reside within the ECM framework
- centralized security policy administration and enforcement
- private certificate authority and X.509 certificate management
- Single Sign On (SSO) and external Light Directory Access Protocol (LDAP) and Remote Authentication Dial In User Service (RADIUS) authentication
- role- and instance-based access control
- local Simple Network Management Protocol (SNMP) management
- central point to manage users, passwords, and system access

Security domain

An ECM security domain is defined by the ECM primary security server. The ECM security domain is comprised of the ECM primary security, the ECM backup security server, and associated member servers that contain the ECM framework and management applications. The primary security server must be the first server deployed in the security domain.

The primary security server is trusted by all servers in the security domain and is based on SSH public key authentication. All the servers in the security domain use the primary security server for authentication, authorization, and audit log storage.

When replication initializes between the backup security server and the primary security server, the backup security server is in a standby mode with the primary security server. When the primary security server is offline, servers in the security domain switch automatically to the backup security server for authentication, authorization, and audit log storage.

Certificate management

ECM uses certificate management: the X.509 certificate for Web Secure Sockets Layer (SSL) for secure communication between a Web browser and a Web server. In CS 1000 Release 5.0, certificates are used for the following:

- Web interfacing using SSL
- Session Initiation Protocol (SIP) signaling using Transport Layer Security (TLS)

Within the ECM security domain, only one private Certificate Authority (CA) is used for CS 1000 to sign internally generated certificates. For certificate management in ECM, a CA is configured only on the primary security server during installation.

When the SIP TLS certificates, signed by the private CA, are distributed to the Network Routing Service or SIP Gateway, the private CA is automatically added to the trusted CA list of the Network Routing Service or SIP Gateway. Therefore, if all the Network Routing Service and SIP Gateway elements use certificates signed by the private CA, mutual authentication for SIP TLS is configured automatically between them.

Secure shell trust of CA

Secure Shell (SSH) is used for the certificate management communication between servers. All servers in the same security domain trust the primary security server where the private CA resides. The Rivest Shamir Adleman (RSA) public key of the primary security server is entered into the authorized key lists of all the servers.

Security framework

The Enterprise Common Manager (ECM) security framework enables element and service management applications to access a common application security infrastructure. The framework manages secure access to Web applications and provides security for Web interfaces and Web utilities.

The ECM security domain provides the central point for Authentication, Authorization, and Auditing (AAA); open, standards-based authentication; and policy-based authorization with a single, unified framework.

ECM provides access to various security features that enable security administrators to configure user and security rights within the application server. Security administrators can create new roles and assign default built-in roles to users within ECM. They can map permissions to a role for each user. Users see only what security administrators authorize them to see based on their assigned roles and permissions.

With ECM, the authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user of ECM.

Access control policies

The authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user of ECM and its managed elements. Authorization supports both Role Based Access Control (RBAC) and Instance Level Access Control (ILAC).

RBAC controls which users have access to protected resources based on user roles. Access rights are grouped by role name, and access to a managed element is restricted to users who are assigned the role name.

ILAC controls which users can apply an operation on a specific instance of a managed element, such as NRS Manager or Element Manager, based on the roles of the user and the permissions of the element granted to the roles. ILAC determines if the request is allowed or denied.

For information about other security changes, including OAM security enhancements, Media Security, Intrasystem signaling security (ISSS) using the IP Security (IPsec) framework, Transport Layer Security (TLS) for Session Initiation Protocol (SIP), and secure signaling using the Secure Multimedia Controller (SMC) 2450, see "Security and Emergency Services" (page 89).

For more information about Enterprise Common Manager, see *Enterprise Common Manager Fundamentals (NN43001-116)*.

Nortel Communication Server 1000

New in this Release

Publication: NN43001-115
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

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

Sourced in Canada