

---

**Nortel Communication Server 1000**

Nortel Communication Server 1000 Release 4.5

---

# **Nortel Communication Server 1000 Element Manager**

## **System Administration**

Document Number: 553-3001-332

Document Release: Standard 5.00

Date: May 2008

---

Copyright © 1994–2008 Nortel Networks. All Rights Reserved.

Sourced in Canada.

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

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

---



---

# Revision history

---

## May 2008

Standard 5.00. This document is up-issued with corrections related to Communication Server 1000 Release 4.5 content as follows:

- QoS Zone Basis Threshold Parameters relationship to QoS Call Basis Threshold Parameters.
- TFS016 QoS IP statistics report information.

## April 2006

Standard 4.00. This document is up-issued with corrections related to Communication Server 1000 Release 4.5 content as follows:

- Note added to page 32 regarding Java Runtime Environment (JRE)
- Note added to page 142 regarding the configuration of elements
- Procedure added to page 159 describing how to load and activate PEP Settings to the Call Server

## August 2005

Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.

## September 2004

Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.

## October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: *Element Management* (553-3023-222). Some content from

*Element Management (553-3023-222) also appears in Succession 1000  
Element Manager: Installation and Configuration (553-3001-232).*

---

# Contents

---

<b>List of procedures</b> .....	<b>9</b>
<b>Introduction</b> .....	<b>11</b>
Contents .....	11
Element Manager overview .....	11
Key features .....	12
Signaling Server .....	13
Call Server and Media Gateway .....	14
IP Line 4,5/Voice Gateway .....	14
<b>About this document</b> .....	<b>17</b>
Subject .....	17
Applicable systems .....	17
Intended audience .....	19
Conventions .....	19
Related information .....	20
<b>How to use Element Manager</b> .....	<b>23</b>
Contents .....	23
Launching Element Manager .....	23
Navigation .....	25
Configuring data .....	29
Logging out .....	29

<b>Links</b> .....	<b>31</b>
Contents .....	31
Introduction .....	31
Virtual Terminals .....	31
Bookmarks .....	35
<b>System</b> .....	<b>39</b>
Contents .....	39
Introduction .....	40
Maintenance .....	40
Loops (Common Equipment) .....	111
Superloops .....	113
SNMP .....	115
Software .....	119
<b>IP Telephony</b> .....	<b>127</b>
Contents .....	127
Introduction .....	128
IP Telephony .....	128
Node Configuration .....	139
Zones .....	146
Network Address Translation (NAT) .....	155
Quality of Service Thresholds (QoS) .....	156
Personal Directories .....	161
Software .....	162
<b>Customers, Routes and Trunks</b> .....	<b>167</b>
Contents .....	167
Introduction .....	167
Customers .....	167
Route and Trunk Configuration .....	177

<b>Dialing and Numbering Plans</b> .....	<b>197</b>
Contents .....	197
Introduction .....	197
Electronic Switched Network .....	198
Network Routing Service and NRS Manager .....	200
Flexible Code Restriction .....	206
Incoming Digit Conversion .....	209
<b>Services</b> .....	<b>213</b>
Contents .....	213
Introduction .....	213
Backup and Restore .....	213
Date and Time .....	223
Logs and Reports .....	225
<b>Security</b> .....	<b>231</b>
Contents .....	231
Introduction .....	231
System Passwords .....	231
PDT Passwords .....	233
Shell Login Options .....	234
SSL/TLS .....	235
Security Alerts .....	235
<b>Certificate Management</b> .....	<b>239</b>
Contents .....	239
Overview .....	240
Creating a new certificate request .....	240
Processing a pending certificate response .....	241
Deleting a pending certificate request .....	242
Creating a self-signed certificate .....	242

Assigning an existing certificate .....	243
Importing a certificate and its private key .....	244
Creating a certificate renew request for the current certificate .....	244
Removing the current certificate .....	245
Replacing the current certificate .....	246
Exporting the current self-signed certificate .....	246
Exporting the current certificate and its private key .....	247
SSL/TSL security configuration .....	248
<b>Support .....</b>	<b>249</b>
Contents .....	249
Introduction .....	249
Help .....	250
Release Notes .....	250
<b>Index .....</b>	<b>251</b>

---

# List of procedures

---

<b>Procedure 1</b>	
<b>Launching Element Manager</b> .....	<b>23</b>
<b>Procedure 2</b>	
<b>Patching of Call Server</b> .....	<b>119</b>
<b>Procedure 3</b>	
<b>Patching of the MG 1000S</b> .....	<b>123</b>
<b>Procedure 4</b>	
<b>Importing node files</b> .....	<b>140</b>
<b>Procedure 5</b>	
<b>Loading and Activating PEP Settings to the Call Server</b> .....	<b>164</b>
<b>Procedure 6</b>	
<b>Adding or editing a Threshold Set Index</b> .....	<b>195</b>
<b>Procedure 7</b>	
<b>Creating a new certificate request</b> .....	<b>240</b>
<b>Procedure 8</b>	
<b>Processing a pending certificate response</b> .....	<b>241</b>
<b>Procedure 9</b>	
<b>Deleting a pending certificate request</b> .....	<b>242</b>
<b>Procedure 10</b>	
<b>Creating a self-signed certificate</b> .....	<b>242</b>

<b>Procedure 11</b>	
<b>Assigning an existing certificate</b> .....	<b>243</b>
<b>Procedure 12</b>	
<b>Importing a certificate and its private key</b> .....	<b>244</b>
<b>Procedure 13</b>	
<b>Creating a certificate renew request</b> .....	<b>245</b>
<b>Procedure 14</b>	
<b>Removing the current certificate</b> .....	<b>245</b>
<b>Procedure 15</b>	
<b>Replacing the current certificate</b> .....	<b>246</b>
<b>Procedure 16</b>	
<b>Exporting the current self-signed certificate</b> .....	<b>246</b>
<b>Procedure 17</b>	
<b>Exporting the current certificate</b> .....	<b>247</b>

---

# Introduction

---

## Contents

This section contains information on the following topics:

<a href="#">Element Manager overview</a> .....	11
<a href="#">Key features</a> .....	12
<a href="#">Signaling Server</a> .....	13
<a href="#">Call Server and Media Gateway</a> .....	14
<a href="#">IP Line 4.5/Voice Gateway</a> .....	14

## Element Manager overview

Element Manager is a resident web-based user interface used to configure and maintain CS 1000 components. Element Manager's web interface enables CS 1000 components to be configured and managed from a web browser.

Element Manager is a simple and user-friendly web-based interface that supports a broad range of system management tasks, including:

- configuration and maintenance of IP Peer and IP Telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks (such as configuration data, customer data, Common Equipment data, D-channels)

- maintenance commands, system status inquiries, backup and restore functions
- software download, patch download, patch activation

Element Manager has many features to help administrators manage systems with greater efficiency. Examples are as follows:

- Web pages provide a single point-of-access to parameters that were traditionally available through multiple overlays.
- Parameters are presented in logical groups to increase ease-of-use and speed-of-access.
- The "hide or show information" option enables administrators to see information that relates directly to the task at hand.
- Full-text descriptions of parameters and acronyms help administrators reduce configuration errors.
- Configuration screens offer pre-selected defaults, drop-down lists, checkboxes, and range values to simplify response selection.

The Element Manager web server resides on the Signaling Server and can be accessed directly through a web browser or Optivity Telephony Manager (OTM). The OTM navigator includes integrated links to each network system and their respective instances of Element Manager.

*Note:* All screen captures in this chapter are applicable to CS 1000S and CS 1000M systems, unless otherwise indicated. In some cases, web pages are different depending on whether they are being presented on a Large or a Small System. Where there is no indicator, the screen and commands are available on both. Where the screen or command is specific to a Large or a Small System, that is indicated.

## Key features

The following functional areas can be accessed using Element Manager:

- **Links** — Provides access to Virtual Terminal sessions and Bookmarks.
- **System** — Provides access to system-wide configuration and basic hardware/software management, including supported maintenance overlays and configuration.

- **IP Telephony** — Helps the user access all functions related to managing IP Telephony. These functions include data and physical structure configuration, high-profile operational activities, and administrative/maintenance functions.
- **Customers** — Allows the user to view and edit customer properties.
- **Routes and Trunks** — Provides access to all functions required to create and manage trunks.
- **Dialing and Numbering Plans** — Used to configure all Electronic Switched Network (ESN) data blocks for the Call Server, as well as to access configuration for the Network Routing Service (NRS). Provides links to NRS Manager, which performs configuration of NRS services, SIP/Re-direct services, and H.323 gatekeeper.
- **Services** — Provides general administrative tools, features and functions, and allows the user to find and access task-related pages, including Security.

## Signaling Server

After software installation and basic configuration of the Signaling Server, components can be configured using the web-based interface. The web server is installed on each Signaling Server within a CS 1000 system. All web pages used by Element Manager are residing on the Signaling Server.

Element Manager enables administrators to perform the following activities on the Signaling Server:

- reset
- access the maintenance window
- download new firmware
- upload new firmware
- view report log
- view Operational Measurements (OM) data
- Telnet

- configure Network Routing Services, including Session Initiation Protocol (SIP) Gateway and Services, SIP/Re-direct server, H.323 Gatekeeper, and associated databases
- increase Virtual Trunk capacity and perform configuration tasks on Virtual Trunks
- configure SNMP community strings and trap destinations for Call Server and Voice Gateway Media Cards, as well as configure the Event Preference Table (EPT) for the Call Server
- configure and manage the web-based services for Personal Directory, Redial List, and Callers List

## Call Server and Media Gateway

For Call Server, Media Gateway 1000S (MG 1000S), and Media Gateway 1000B (MG 1000B), Element Manager enables administrators to configure and manage the following data:

- Configuration Record
  - Supports ADAN, CEQU, PWD, and SUPL data blocks
- Customer Data Block
  - Supports ANI, FCR, FTR, LDN, NET, and NIT data blocks
- Route Data Blocks
- Trunks
- ESN Data Block

To learn more about parameters that can be configured and managed in Element Manager, see *System Management* (553-3001-300).

## IP Line 4.5/Voice Gateway

Element Manager enables administrators to perform the following activities on the IP Line 4.5/Voice Gateway Media Cards:

- View and configure Simple Network Management Protocol (SNMP) parameters and add IP addresses for forwarding SNMP traps.

- View and configure Voice Gateway profile data.
- View and edit Quality of Service (QoS) parameters.
- Use Local Area Network (LAN) configuration to configure the Management LAN (ELAN) subnet, Telephony LAN (TLAN) subnet, and Routes.
- View and edit Simple Network Transfer Protocol (SNTP) Server and Client information.
- View and configure file server access for downloading firmware for IP Phones.
- View and select the Loss and Level Plan for the country. For more information about selecting the Loss and Level Plan for the country, see *Transmission Parameters* (553-3001-182).
- Add, remove, view, and edit card properties of Voice Gateway Media Cards.
- Add, remove, view, and edit Signaling Server information.

To learn more about IP Line 4.5 and Voice Gateway Media Card parameters that can be configured and managed in Element Manager, see *IP Line: Description, Installation, and Operation* (553-3001-365).

The following maintenance activities are supported using Element Manager for IP Line 4.5 and Voice Gateway Media Card:

- reset Voice Gateway Media Card
- enable/Disable Voice Gateway Media Card
- access the maintenance window to the Voice Gateway Media Card
- download new loadware/firmware for upgrades
- run Syslog reports
- obtain Operational Measurement (OM) data
- Telnet to the card

To learn more about IP Line 4.5 and Voice Gateway maintenance activities that are supported by Element Manager, see “Superloops” on [page 113](#).



## About this document

---

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

### Subject

This Nortel Technical Publication (NTP) is a reference tool for Communication Server 1000 Element Manager, a web-based interface that enables configuration, maintenance, upgrade, and patching functions. This document describes the interface and its related functionality.

#### **Note on legacy products and releases**

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

[www.nortel.com](http://www.nortel.com)

### Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

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

### System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.5 software and configured to include a Signaling Server, they become CS 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

**Table 1**  
**Meridian 1 systems to CS 1000M systems**

<b>This Meridian 1 system...</b>	<b>Maps to this CS 1000M system</b>
Meridian 1 PBX 11C Chassis	CS 1000M Chassis
Meridian 1 PBX 11C Cabinet	CS 1000M Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81	CS 1000M Multi Group
Meridian 1 PBX 81C	CS 1000M Multi Group

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

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures (553-3011-258)*
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures (553-3021-258)*
- *Communication Server 1000S: Upgrade Procedures (553-3031-258)*
- *Communication Server 1000E: Upgrade Procedures (553-3041-258)*

## Intended audience

This document is intended for individuals responsible for system administration using Element Manager.

## Conventions

### Terminology

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

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

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

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

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

- Communication Server 1000M Half Group (CS 1000M HG)

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

## Related information

This section lists information sources that relate to this document.

### NTPs

The following NTPs are referenced in this document:

- *What's New for Communication Server 1000 Release 4.5* (553-3001-015)
- *Signaling Server: Installation and Configuration* (553-3001-212)
- *IP Peer Networking: Installation and Configuration* (553-3001-213)
- *Branch Office: Installation and Configuration* (553-3001-214)
- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230)
- *System Management* (553-3001-300)
- *Software Input/Output: Administration* (553-3001-311)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Software Input/Output: Maintenance* (553-3001-511)
- *Simple Network Management Protocol: Description and Maintenance* (553-3001-519)
- *Communication Server 1000S: Overview* (553-3031-010)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)
- *Communication Server 1000S: Maintenance* (553-3031-500)

### **Online**

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

[www.nortel.com](http://www.nortel.com)

### **CD-ROM**

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



---

# How to use Element Manager

---

## Contents

This section contains information on the following topics:

Launching Element Manager .....	23
Time-out after a period of inactivity .....	25
Navigation .....	25
Configuring data .....	29
Logging out .....	29

## Launching Element Manager

To log in to Element Manager, follow the steps in Procedure 1. Element Manager supports Microsoft™ Internet Explorer 6.0.2600 for Windows operating systems.

Before following this procedure, see *Signaling Server: Installation and Configuration* (553-3001-212) for information about setting up a browser for optimal performance of Element Manager.

**Note:** This procedure requires Service Pack 1 and Java Runtime environment.

### Procedure 1 Launching Element Manager

- 1 Open the web browser.

- 2 Enter the **Signaling Server Node IP address** in the Address Bar of the browser window, and press **Enter** on the keyboard.

**Note:** The ELAN network interface IP address may be required, instead of the Node IP address, to access the Element Manager login web page in secure environments.

- 3 Element Manager opens with the **Login** web page (see Figure 1).

**Note:** If a security certificate has been correctly installed, and the usage rule set to “UserChoice”, the user will have the option of logging in using Secure mode. If the usage rule is set to “Always”, the user will be redirected to the https site, and a warning message will appear. For more information, see “Certificate Management” on [page 239](#).

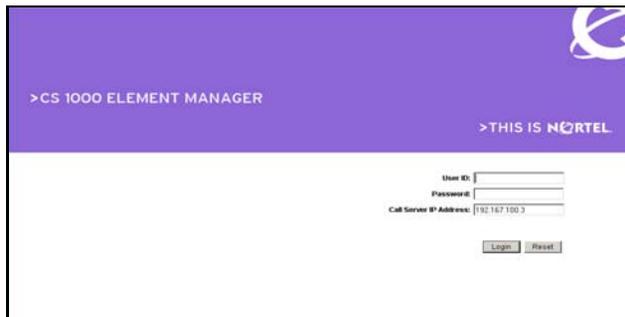
- a. Enter a valid **User ID** and **Password** combination.

**Note:** A valid **User ID** and **Password** combination is one that is defined on the Call Server.

The IP Address of the Call Server appears in the **Call Server IP Address** field.

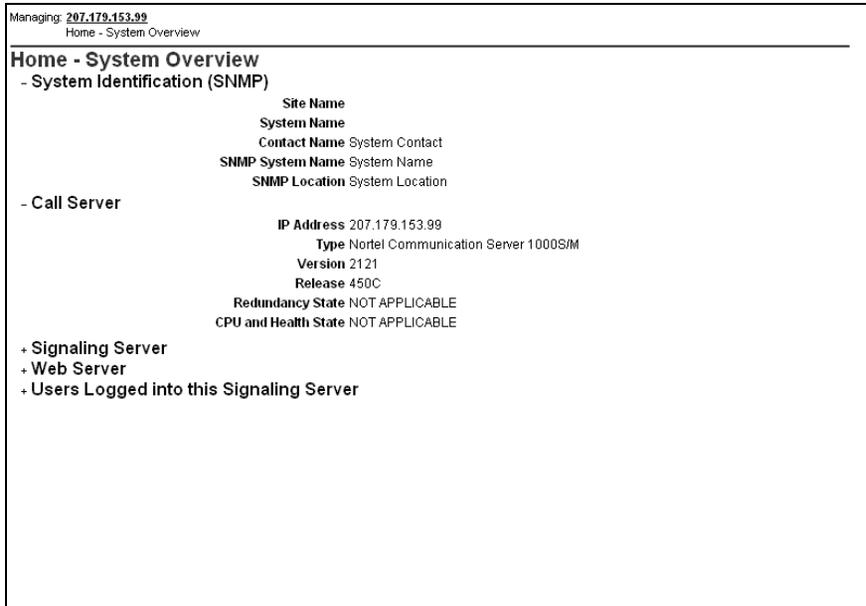
- b. Click the **Login** button.

**Figure 1**  
**Element Manager–Login web page**



- 4 The **System Overview** web page opens (see Figure 2 on [page 25](#)).

**Figure 2**  
**Element Manager System Overview web page**



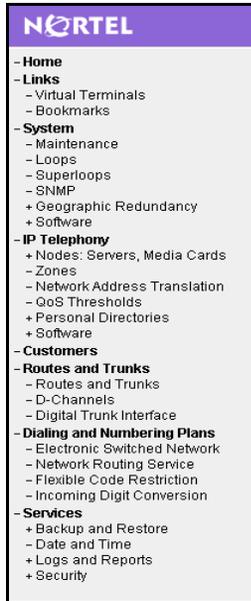
## Time-out after a period of inactivity

Element Manager times out after a period of inactivity. Users are logged out without any warning in all Element Manager web pages. The exception to this is the Node Configuration **Edit** web pages. When working in this web page, a message is displayed that warns of the impending time-out action. Click the **OK** button (on the warning message) within the remaining time-out period (five minutes) to reset the timer. If there is no response within the five-minute warning period, the session is cancelled and the user must log in again. Any data modifications made on screen, but not submitted to the system, are lost.

## Navigation

The Element Manager navigator is located on the left side of the browser window, as shown in Figure 3 on [page 26](#).

**Figure 3**  
**Element Manager navigator**



Links in the navigator are structured as follows:

- **Home**
- **Links**
  - Virtual Terminals
  - Bookmarks
- **System**
  - Maintenance
  - Loops
  - Superloops
  - SNMP
  - Geographic Redundancy (Large System only)

- Database Replication Control
  - State Control
- Software
  - Call Server
  - Media Gateway
- **IP Telephony**
  - Nodes: Servers, Media Cards
    - Maintenance and Reports
    - Configuration
  - Zones
  - Network Address Translation
  - QoS Threshold
  - Personal Directories
    - Server
    - User Profile
    - Backup and Restore
  - Software
    - File Upload
    - Voice Gateway Media Card
    - Telephony Firmware
    - Servers and Media Cards
- **Customers**
- **Routes and Trunks**
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface

- **Dialing and Numbering Plans**
  - Electronic Switched Network
  - Network Routing Service
  - Flexible Code Restriction
  - Incoming Digit Conversion
  
- **Services**
  - Backup and Restore
    - Call Server
    - Personal Directories
  - Date and Time
  - Logs and Reports
    - IP Telephony Nodes
    - Call Server Report Utility
    - Equipped Feature Packages
    - Peripheral Software Version Data
    - System Licence Parameters
  - Security
    - System Passwords
    - PDT Passwords
    - Shell Login Options
    - SSL/TLS

During periods of high call volume, Element Manager web pages load more slowly.

## Configuring data

In many cases, users can edit data via configuration web pages. At the bottom of the configuration web pages, the following four buttons appear:

- **Submit** — Transmits changes to the Call Server.
- **Refresh**— Refreshes data from the Call Server. Refresh overwrites any changes not yet submitted.
- **Delete** — Deletes the item being edited or configured.
- **Cancel** — Discards the changes and returns to the appropriate configuration page.

## Logging out

To log out of Element Manager, click the **Logout** link in the top right-hand corner.



### **WARNING**

Do not close the browser window before logging out. The session will remain active and the user will be unable to log in again.



---

# Links

---

## Contents

This section contains information on the following topics:

<a href="#">Introduction</a> . . . . .	31
<a href="#">Virtual Terminals</a> . . . . .	31
<a href="#">Bookmarks</a> . . . . .	35

## Introduction

The features available under the **Links** branch of the Element Manager navigator enable Element Manager to be the single point of management access to web pages and character-based interfaces.

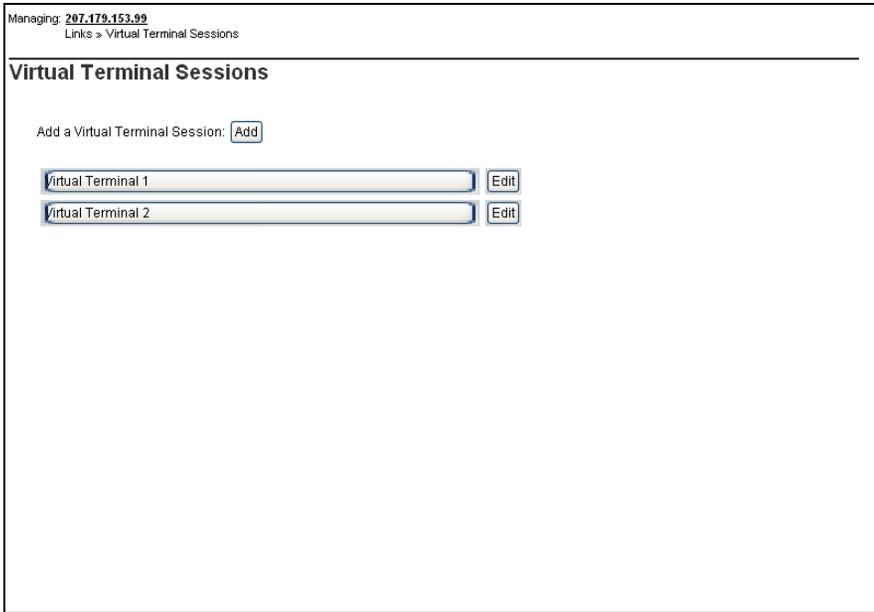
Use the Virtual Terminal feature to define and access the IP addresses of any character-based interfaces. On the Call Server, users can access context-sensitive online help, which provides detailed information on system prompts and error messages.

The Bookmarks feature allows access to any web servers embedded within the system's components. Users can also add links to any other useful web sites.

## Virtual Terminals

Click the **Virtual Terminals** link to open the **Virtual Terminal Sessions** web page as shown in [Figure 4 on page 32](#).

**Figure 4**  
**Virtual Terminal Sessions web page**



The **Virtual Terminal Sessions** web page enables users to Telnet to any IP-based element in the system. By entering and saving the IP address to Telnet to a particular IP-based element, users can access those elements more quickly in the future.

**Note:** Java Runtime Environment (JRE) version 1.5 must be installed for the Virtual Terminal Emulator to run properly.

To add a new Virtual Terminal Session, do the following:

- 1 On the **Virtual Terminal Sessions** web page, click the **Add** button. The **Virtual Terminal Session Property Configuration** web page opens, as shown in [Figure 5](#).

**Figure 5**  
**Virtual Terminal Sessions Property Configuration web page**

Managing: 207.179.153.99  
Links > Virtual Terminal Sessions > Virtual Terminal Session Property Configuration

### Virtual Terminal Session Property Configuration

Input Description	Input Value
Description	<input type="text"/>
IP Address	<input type="text"/>
Call Server	<input type="checkbox"/>

- 2 Enter a description and IP Address for the session.
- 3 If creating a Virtual Terminal Session to a Call Server, select the Call Server check box.
- 4 Click **Submit** to save. To cancel the session, click **Cancel**.

To access a Virtual Terminal Session that has already been created, click the name of the Virtual Terminal Session on the **Virtual Terminal Sessions** web page. A **Virtual Terminal** window opens in a separate browser window.

The Virtual Terminal window provides a menu with the following items:

- Current Overlay
- Current Prompt
- Last System Message
- Search M1 Help Files
- About Terminal Client

When the user enters an overlay, the Current Overlay and Current Prompt menu items are enabled.

Click the **Help -> Current Overlay** link to open a Help window containing help for that particular overlay.

Click the **Help -> Current Prompt** link to open a Help window explaining the definition of the prompt, along with acceptable responses.

Click the **Help -> Last System Message** link to open a Help window for system messages when wrong input is given.

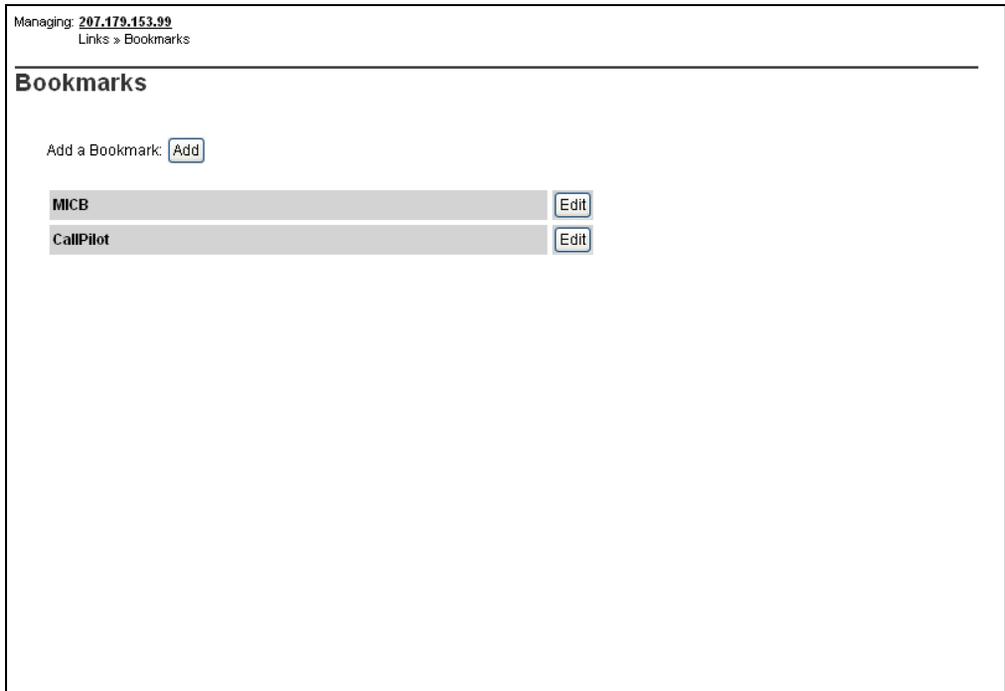
To edit an existing Virtual Terminal session, do the following:

- 1 Click **Edit** next to the name of the Virtual Terminal Session. The information about the Virtual Terminal Session selected is displayed in the fields. Edit the Description and IP Address values.
- 2 If changing this session so that it now logs into a Call Server, then select the Call Server check box.
- 3 Click **Submit** to record the changes. Click **Delete** to remove the Virtual Terminal Session information completely. Click **Cancel** to disregard any changes made.

## Bookmarks

Element Manager enables users to bookmark web sites for easy access. Click the **Bookmarks** link to open the **Bookmarks** web page, as shown in [Figure 6](#).

**Figure 6**  
**Bookmarks web page**



To create a new bookmark, do the following

- 1 Click the **Add** button next to **Add a Bookmark**. The **Bookmark Property Configuration Page** opens, as shown in [Figure 7](#).

**Figure 7**  
**Bookmark Property Configuration web page**

Managing: [207.179.153.99](#)  
Links > [Bookmarks](#) > Bookmark Property Configuration

### Bookmark Property Configuration

Input Description	Input Value
Description	<input type="text"/>
Location	<input type="text" value="http://"/>

- 2 Enter a **Description** and **Location** (the URL) of the web site to be bookmarked.
- 3 Click **Submit** to enter the bookmark. To cancel the session, click **Cancel**.

To access a bookmark that has already been created, click on the name of the bookmark on the **Bookmark** web page. The web site opens.

To edit the properties of an existing bookmark, do the following

- 1 Click the **Edit** button next to the name of the bookmark on the **Bookmarks** web page. The **Bookmark Property Configuration** window opens, as shown in [Figure 8](#).

**Figure 8**  
**Bookmark Property Configuration web page - Edit**

Managing: [207.179.153.99](#)  
Links > [Bookmarks](#) > Bookmark Property Configuration

### Bookmark Property Configuration

Input Description	Input Value
Description	<input type="text" value="CallPilot"/>
Location	<input type="text" value="http://207.179.153.100"/>

- 2 The information about the selected bookmark is displayed. Edit the **Description** and **Location** (URL) values.
- 3 Click **Submit** to record the changes. Click **Delete** to remove the bookmark completely. Click **Cancel** to disregard any changes made.



---

# System

---

## Contents

This section contains information on the following topics:

Introduction . . . . .	40
Maintenance . . . . .	40
Application Module Link Diagnostics . . . . .	45
Background Signaling and Switching Diagnostics . . . . .	47
Call Trace Diagnostics . . . . .	49
Clock Controller Diagnostics . . . . .	53
Core Common Equipment Diagnostics . . . . .	55
Core Input/Output Diagnostics . . . . .	61
D-channel Diagnostics . . . . .	64
D-Channel Expansion Diagnostics . . . . .	66
Digital Trunk Diagnostics . . . . .	68
Digital Trunk Maintenance Diagnostics . . . . .	73
Ethernet Diagnostics . . . . .	75
Ethernet Quality of Service Diagnostics . . . . .	79
Event Preference Table (EPT) . . . . .	81
Input/Output Diagnostics . . . . .	82
Intergroup Switch and System Clock Generator Diagnostics . . . . .	85
MSDL Diagnostics . . . . .	89
Multifrequency Sender Diagnostics . . . . .	91
Multifrequency Signaling Diagnostics . . . . .	93
Network and Peripheral Equipment Diagnostics . . . . .	95
Network and Signaling Diagnostics . . . . .	101
TMDI Diagnostics . . . . .	103

Tone and Digit Switch Diagnostics .....	105
Trunk Diagnostics .....	107
Zone Diagnostics .....	109
Loops (Common Equipment) .....	111
Superloops .....	113
SNMP .....	115
Geographic Redundancy.....	116
Software .....	119
Call Server .....	119
Media Gateway .....	123

## Introduction

The **System** branch of the Element Manager navigator provides access to diagnostic tools that enable users to issue a variety of commands to the components of the CS 1000 system.

The following buttons appear on some or all of the System web pages:

- **Submit** — Transmits changes to the Call Server.
- **Refresh**— Refreshes data from the Call Server. Refresh overwrites any changes not yet submitted.
- **Cancel** — Discards the changes and returns to the appropriate configuration web page.

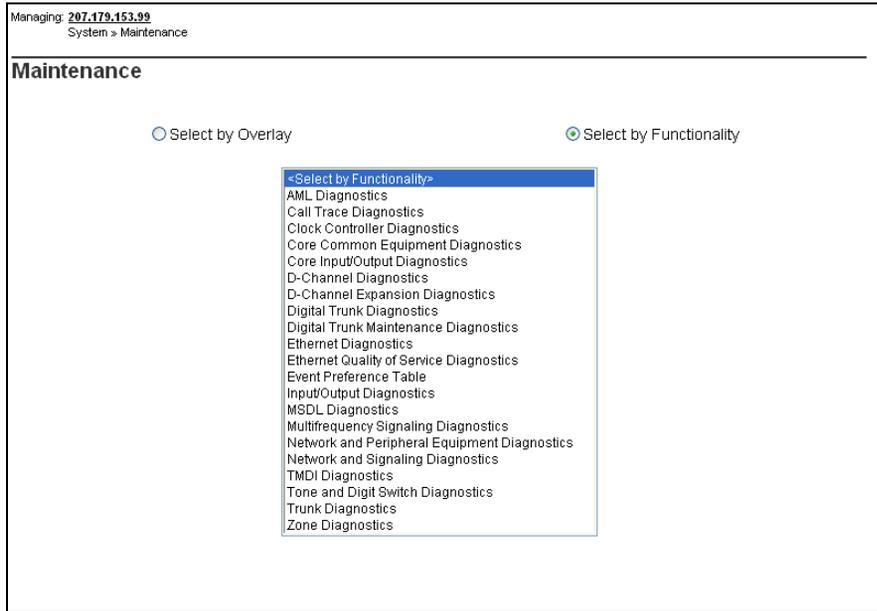
The diagnostic tools and system status information available through this branch of the navigator are divided into five major categories: **Maintenance**, **Loops**, **Superloops**, **SNMP**, and **Software**.

## Maintenance

When the user clicks the **Maintenance** link in the **System** branch of the Element Manager navigator, the **Maintenance** web page opens. The user can choose how the options are presented. If choosing **Select by Functionality**,

the diagnostic tool options are presented by functionality as shown in [Figure 9](#).

**Figure 9**  
**Maintenance diagnostic tools presented by functionality**



The following tool options are available from this web page:

- AML Diagnostics
- Call Trace Diagnostics
- Clock Controller Diagnostics
- Core Common Equipment Diagnostics
- Core Input/Output Diagnostics
- D-Channel Diagnostics
- D-Channel Expansion Diagnostics
- Digital Trunk Diagnostics

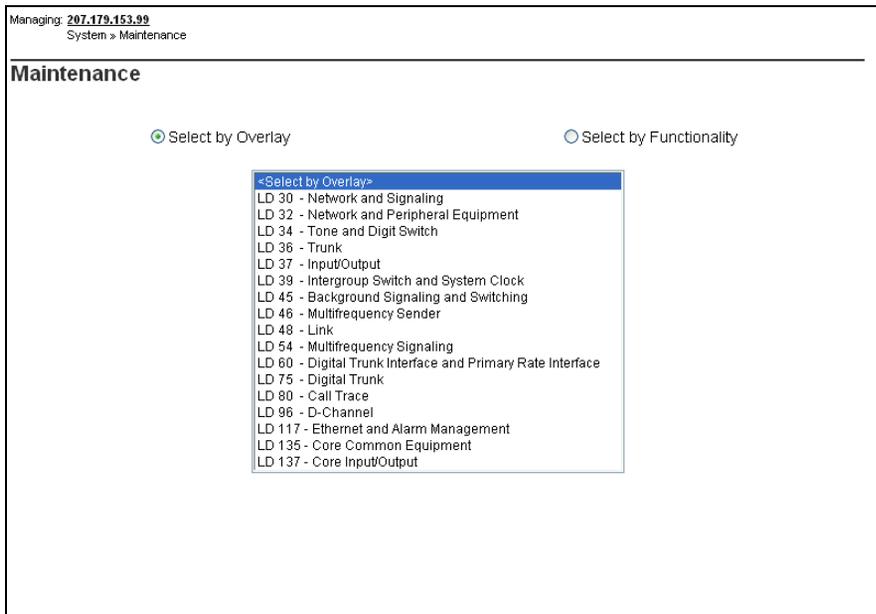
- Digital Trunk Maintenance Diagnostics
- Ethernet Diagnostics
- Ethernet Quality of Service Diagnostics
- Event Preference Table
- Input/Output Diagnostics
- MSDL Diagnostics
- Multifrequency Signaling Diagnostics
- Network and Peripheral Equipment Diagnostics
- Network and Signaling Diagnostics
- TMDI Diagnostics
- Tone and Digit Switch Diagnostics
- Trunk Diagnostics
- Zone Diagnostics

If choosing **Select by Overlay**, the following options are presented by LD numbers, as shown in [Figure 10 on page 43](#):

- LD 30 - Network and Signaling
- LD 32 - Network and Peripheral Equipment
- LD 34 - Tone and Digit Switch
- LD 36 - Trunk
- LD 37 - Input/Output
- LD 39 - Intergroup Switch and System Clock
- LD 45 - Background Signaling and Switching
- LD 46 - Multifrequency Sender
- LD 48 - Link
- LD 54 - Multifrequency Signaling

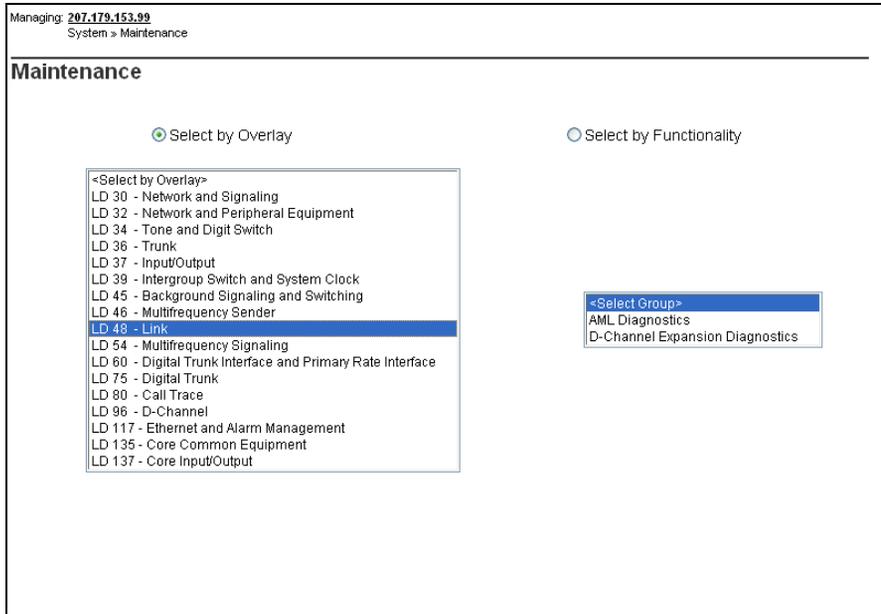
- LD 60 - Digital Trunk Interface and Primary Rate Interface
- LD 75 - Digital Trunk
- LD 80 - Call Trace
- LD 96 - D-Channel
- LD 117 - Ethernet and Alarm Management
- LD 135 - Core Common Equipment
- LD 137 - Core Input/Output

**Figure 10**  
**Call Server diagnostic tools presented by overlay**



If selecting an overlay that corresponds to more than one functionality, choose the desired functionality in the **Select Group** drop-down list, as shown in [Figure 11 on page 44](#).

**Figure 11**  
**Select Group drop-down list**



This document presents the options by functionality, with cross-references to the appropriate overlay.

The following sections provide information on each functionality.

## Application Module Link Diagnostics

Click the **AML Diagnostics** link in the list of **Maintenance** functionalities to open the **Link: AML Diagnostics** web page, as shown in [Figure 12](#).

**Figure 12**  
**AML Diagnostics web page**

Managing: [207.179.153.99](#)  
System > [Maintenance](#) > Link: AML Diagnostics

---

**Link: AML Diagnostics**

Diagnostic Commands	Command Parameters	Action
STAT AML - Get AML status	<input type="text"/> (device #)	<input type="button" value="Submit"/>
DIS AML - Disable AML	<input type="text"/> (device #)	<input type="button" value="Submit"/>
ENL AML - Enable AML	<input type="text"/> (device #)	<input type="button" value="Submit"/>

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

The commands available from this web page correspond to the AML diagnostics traditionally performed using LD 48.

To perform AML commands on this web page, do the following:

Select one of the following commands from the first **Commands** drop-down list:

- a STAT AML - Get AML status
- b STAT ELAN - Check status of all specified/ all configured ELANs
- c EST AML - Establish layer 2 on AML
- d MAP AML - Get card information of one or all AMLs

- e RLS AML - Release layer 2 on AML
- f SLFT AML - Perform self-test on AML
- g UPLD AML - Upload parameter table 1 to 4 from AML

- 1 Enter the device number in the **Commands Parameters** text box.
- 2 Click the **Submit** button.

To disable AML using this web page, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a DIS AML - Disable AML
  - b DIS AML - Disable AUTO recovery on AML
  - c DIS AML - Disable layer 2 on AML
  - d DIS AML - Disable layer 7 on AML
  - e DIS AML - Disable MDL error reporting on AML
  - f DIS ELAN - Disable ELAN (server/client task)
- 2 Enter the device number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To enable AML using this web page, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a ENL AML - Enable AML
  - b ENL AML - Enable Automatic set-up on AML
  - c ENL AML - Enable AUTO recovery on AML
  - d ENL AML - Enable Layer 2 on AML
  - e ENL AML - Enable Layer 7 on AML
  - f ENL AML - Enable MDL error reporting on AML
  - g ENL ELAN- Enable ELAN (server task)

- 2 Enter the device number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

## Background Signaling and Switching Diagnostics

The **Background Signaling and Switching diagnostics** web page is applicable only to Large Systems.

Click the **Background Signaling and Switching** link in the list of **Call Server** functionalities to open the **Background Signaling and Switching Diagnostics** web page, as shown in [Figure 13](#).

**Figure 13**  
**Background Signaling and Switching Diagnostics web page**

Managing: [192.167.100.3](#)  
System » [Maintenance](#) » Background Signaling and Switching Diagnostics

### Background Signaling and Switching Diagnostics

Diagnostic Commands	Command Parameters	Action
TEST - Perform continuity test for specified (all) loops	(loop/none)	Submit

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

Cancel

The commands available from this web page correspond to the Background Signaling and Switching command traditionally performed using LD 45 - Background Signaling and Switching Diagnostics.

This web page is used to perform the TEST command. This command performs a continuity test for specified loops. Enter the loop number in the **Command Parameters** box. To run the TEST command on all loops, leave the Command Parameters box empty. Then click **Submit**.

## Call Trace Diagnostics

Click the **Call Trace Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Call Trace Diagnostics** web page. On a Small System, the web page appears as shown in [Figure 14](#).

**Figure 14**  
Call Trace Diagnostics web page - Small System

Managing: 207.179.153.99  
System > Maintenance > Call Trace Diagnostics

---

### Call Trace Diagnostics

Diagnostic Commands	Command Parameters	Action
TRAC - List Route, type and status of trunks for a Customer	<input type="text"/> (cust# acod#)	<input type="button" value="Submit"/>
TRAD - Trace digital calls on a channel of specified card	<input type="text"/> (card# ch#)	<input type="button" value="Submit"/>
TRAT - Trace calls for an attendant of a customer	<input type="text"/> (cust# attnd#)	<input type="button" value="Submit"/>
TRAK - Trace calls associated with the unit	<input type="text"/> (c u)	<input type="button" value="Submit"/>
TRAO - Trace Attendant calls associated with the unit	<input type="text"/> (c u) <input type="checkbox"/> DEV	<input type="button" value="Submit"/>

---

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

The commands available from this web page correspond to the Call Trace diagnostics traditionally performed using LD 80 - Call Trace Diagnostics.

On a Small System, this web page is used to perform the following Call Trace functions.

To perform TRAC commands, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a TRAC - List Route, type and status of trunks for a Customer
  - b TRAC - Trace calls for specified customer and DN/LSC DN
  - c TRAC - Trace calls for specified customer, route and member
- 2 Enter the customer number and the acod number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To perform TRAD commands, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a TRAD - Trace digital calls on a channel of a specified card
  - b TRAD - Trace DTI calls on a channel of specified loop
- 2 Enter the card number and channel number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To perform TRAT commands, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a TRAT - Trace calls associated with the specified unit
  - b TRAT - Trace calls on a key of an attendant of a customer
- 2 Enter the card number and attendant number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To perform TRAK commands, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a TRAK - Trace calls associated with the unit
  - b TRAK - Trace calls on a specified key for the unit
- 2 Enter the required parameters in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To perform TRAO commands, do the following:

- 1 Select one of the following commands from the fifth **Commands** drop-down list:
  - a TRAO - Trace Attendant calls associated with the unit
  - b TRAO - Trace Attendant calls for specified key for the unit.
- 2 Enter the required parameters in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

On a Large System, this web page appears as shown in [Figure 15 on page 52](#).

**Figure 15**  
**Call Trace Diagnostics web page - Large System**

Managing: **192.167.100.3**  
System > [Maintenance](#) > Call Trace Diagnostics

---

### Call Trace Diagnostics

Diagnostic Commands	Command Parameters	Action
TRAC - List Route, type and status of trunks for a Customer	<input type="text"/> (cust# acod#) <input type="checkbox"/> DEV	Submit
TRAD - Trace DTI/DLI calls on a channel of a loop	<input type="text"/> (loop# ch#)	Submit
TRAT - Trace calls for an attendant of a customer	<input type="text"/> (cust# atnd#) <input type="checkbox"/> DEV	Submit

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

The web page is used to perform the following Call Trace functions.

To perform TRAC commands, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a TRAC - List Route, type and status of trunks for a Customer
  - b TRAC - Trace calls for a specified customer and DN/LSC DN
  - c TRAC - Trace calls for a specified customer, route and member
  - d TRAC - Trace calls on specified Digital Subscriber Loop(0-7)
  - e TRAC - Trace calls associated with the specified unit
  - f TRAC - Trace calls on specified key for specified unit

- 2 Enter the customer number and the acod number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To perform TRAD commands, do the following:

- 1 Select TRAD - Trace DTI/DLI calls on a channel of a loop in the second **Commands** drop-down list:
- 2 Enter the loop number and channel number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To perform TRAT commands, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a TRAT - Trace calls for an attendant of a customer
  - b TRAT - Trace calls on a key of an attendant of a customer
  - c TRAT - Trace attendant calls for a unit
  - d TRAT - Trace attendant calls on specified key of a unit
- 2 Enter the customer number and attendant number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

## Clock Controller Diagnostics

Click the **Clock Controller Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Digital Trunk Interface and Primary Rate Interface: Clock Controller Diagnostics** web page, as shown in [Figure 16 on page 54](#).

**Figure 16**  
**Digital Trunk Interface and Primary Rate Interface: Clock Controller Diagnostics web page**

Managing: **192.167.100.3**  
 System > [Maintenance](#) > Digital Trunk Interface and Primary Rate Interface :Clock Controller Diagnostics

---

**Digital Trunk Interface and Primary Rate Interface :Clock Controller Diagnostics**

Action:  FULL  In Side

Card Status	Clock State	Clock Controller	Group	Side	Primary Reference	Secondary Reference	Auto Switch Clock	Cabinet Clock Source	Error				
<table border="1"> <thead> <tr> <th>IP DB Port</th> <th>Port Status</th> </tr> </thead> <tbody> <tr> <td colspan="2"> <p>DTI207:            No clock has been found in side S. This indicates that either there is no clock in side S or the clock in side S has its shelf-side switch set wrong.</p> <p>SEVERITY: Info</p> </td> </tr> </tbody> </table>										IP DB Port	Port Status	<p>DTI207:            No clock has been found in side S. This indicates that either there is no clock in side S or the clock in side S has its shelf-side switch set wrong.</p> <p>SEVERITY: Info</p>	
IP DB Port	Port Status												
<p>DTI207:            No clock has been found in side S. This indicates that either there is no clock in side S or the clock in side S has its shelf-side switch set wrong.</p> <p>SEVERITY: Info</p>													

This web page is used to maintain the digital trunk interface and primary rate interface clock controllers.

The commands available from this web page correspond to the Clock Controller data traditionally maintained using LD 60- Digital Trunk Interface and Primary Rate Interface Clock Controller.

This web page shows the status of the Clock Controller card. If using a Small System, the status of the IP daughterboard ports is shown.

To perform maintenance activities on a Small System using this web page:

- 1** Select one of the following commands from the **Action** drop-down list:
  - a** SSCK - Get Status of the Clock
  - b** ENL CC - Enable the Clock
  - c** DIS CC - Disable the Clock

- d TRCK - Set the Clock Controller
  - e ENCK - Enable the secondary clock reference for card
  - f DNCK - Disable the secondary clock reference for card
- 2 Select a Cabinet number from the **In Cabinet** drop-down list.
  - 3 Click the **Submit** button.

To perform maintenance activities on a Large System using this web page:

- 1 Select one of the following commands from the **Action** drop-down list.
  - a SSCK - Get Status of the Clock
  - b ENL CC - Enable the Clock
  - c DIS CC - Disable the Clock
  - d TRCK - Set the Clock Controller
  - e DSCK - Disable the clock for loop
  - f ENCK - Enable the clock for loop
  - g EREF - Enable auto switchover of reference clocks
  - h IDC - Get card ID of Clock Controller card
  - i MREF - Disable switchover of system clocks
  - j SEFT CC - Execute self test
- 2 Select the Core number (Core 0 or Core 1) from the **In Side** drop-down list.
- 3 Click the **Submit** button.

## Core Common Equipment Diagnostics

The commands available on the **Core Common Equipment Diagnostics** web page vary depending on whether the user is working with a Large System or a Small System.

On a Small System, click the **Core Common Equipment Diagnostics** link in the list of **Maintenance** functionalities to open the **Core Common Equipment Diagnostics** web page, as shown in Figure 17 on [page 56](#).

**Figure 17**  
**Core Common Equipment Diagnostics web page - Small System**

Managing: [207.179.153.99](#)  
System » Maintenance » Core Common Equipment Diagnostics

### Core Common Equipment Diagnostics

Diagnostic Commands	Command Parameters	Action
STAT CPU - Status of the CPU card	(none)	Submit
ENL FIL - Enable Fiber Optic Link	(link#)	Submit
LLBK FIL - Local Loopback Test on Fiber optic Link	(link#)	Submit
LOCK - Lock IP Expansion cabinet/Media Gateway	(cabinet#)	Submit

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

Cancel

This web page is used to maintain Core Common Equipment on the Small System. The commands available from this web page correspond to data traditionally maintained using LD 135 - Core Common Equipment Diagnostic.

To obtain status information using this web page on a Small System, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT CPU - Status of the CPU card
  - b STAT MAC - MAC Address of IP DBs on SSC Card
  - c STAT FIL - Status of all(specific) Links
  - d STAT MEM - Status of SIMMS on both CPUs
- 2 Click the **Submit** button.

To execute commands on Fiber links using this web page, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a ENL FIL - Enable Fiber Optic Link
  - b DIS FIL - Disable Fiber Optic Link
- 2 Enter the link number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To execute loopback commands using this web page, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a LLBK FIL - Local Loopback Test on Fiber optic link
  - b LLBK IP - Local Loopback Test on IP Connectivity link
  - c RLBK FIL - Remote Loopback Test on Fiber optic link
- 2 Enter the link number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

To execute cabinet commands using this web page, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a LOCK - Lock IP Expansion cabinet/Media Gateway
  - b UNLOCK - Unlock IP Expansion cabinet/Media Gateway
  - c SOTS - Switch over to Survivable mode
  - d SBFS - Switch back from Survivable mode
- 2 Enter the cabinet number in the **Commands Parameters** text box.
- 3 Click the **Submit** button.

On a Large System, click the **Core Common Equipment Diagnostics** link in the list of **Maintenance** functionalities to open the **Core Common Equipment Diagnostics** web page, as shown in [Figure 18 on page 58](#).

**Figure 18**  
**Core Common Equipment Diagnostic web page - Large System**

Managing: **192.167.100.3**  
 System > Maintenance > Core Common Equipment Diagnostics

---

### Core Common Equipment Diagnostics

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

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

Cancel

To execute status commands using this web page, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT CPU - Core status for both CPUs
  - b STAT CNI - Status of configured CNI(c=side, s=slot, p=port)
  - c STAT MEM - Status of SIMMs on both CPs
  - d STAT EXT - Status of all Extender pair designations
  - e STAT SUTL - Status of system utility

To execute CNI commands using this web page, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a ENL CNI - Enable CNI card/port (c=side, s=side, p=port)
  - b DIS CNI - Disable CNI all,card or port
  - c DSPL - Display active core contents
  - d DSPL ALL - Display active core contents for all
  - e IDC CPU - Print card ID for active core
  - f IDC CNI - Print card ID for CNI on active side
  - g ENL EXT - Enable specified Extender pair
- 2 Enter the required parameters in the **Commands Parameters** text box. The required parameters are found next to the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute test commands using this web page, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a TEST CPU - Test the inactive core
  - b TEST CNI - Test CNI card/port(c=card, s=slot, p=port)
  - c TEST IPB - Test backplane on Secondary Interprocessor Bus
  - d TEST LCD - Test the LCD display on the active CP card
  - e TEST LED - Test LEDs
  - f TEST SUTL - Test system utility
- 2 Click the **Submit** button.

To execute miscellaneous commands using this web page, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a SCPU - Switch cores
  - b SPLIT - Put a redundant system into single mode
  - c CDSP - Clear maintenance displays
  - d CMAJ - Clear major alarm and reset power fail transfer
  - e CMIN - Clear the minor lamp on a system basis
  - f CMIN ALL - Clear minor alarm on all attendant consoles
  - g CUTOVR - Transfer call processing from active to standby cores
  - h JOIN - Synchronize the memory and drives
- 2 Click the **Submit** button.

To execute status health commands using this web page, do the following:

- 1 Select one of the following commands from the fifth **Commands** drop-down list:
  - a STAT HEALTH HELP - Help for health commands
  - b STAT HEALTH - Overall health status
  - c STAT HEALTH AML - AML health status
  - d STAT HEALTH IPL - IPL health status
  - e STAT HEALTH ELAN - ELAN health status
  - f STAT HEALTH HW - Hardware health status
- 2 Click the **Submit** button.

To execute Geographic Redundancy commands using this web page, do the following:

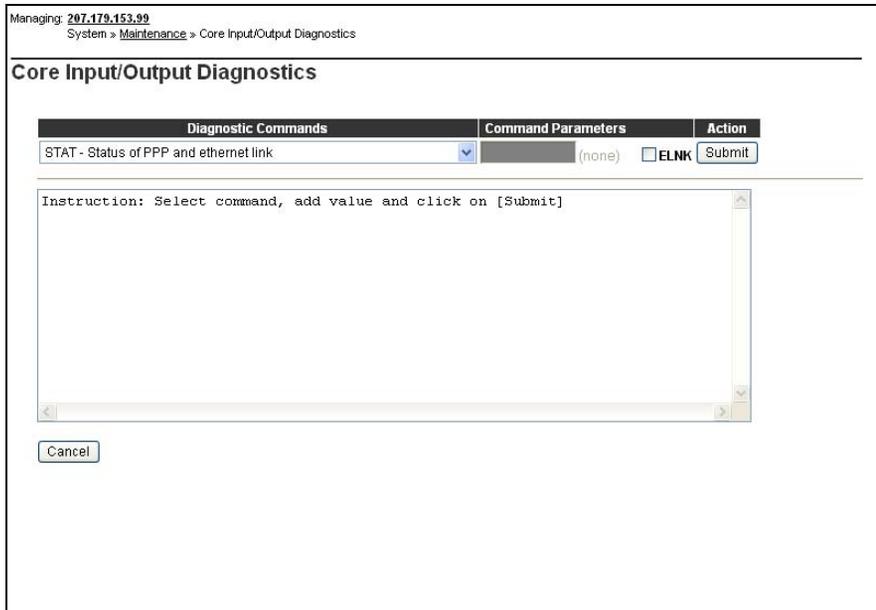
- 1 Select one of the following commands from the sixth **Commands** drop-down list:
  - a STAT GR - Status of Geographic Redundancy
  - b TEST GR - Test Geographic Redundancy
  - c CLR GR - Clear operation for the secondary CS
- 2 Click the **Submit** button.

## Core Input/Output Diagnostics

When the user clicks the **Core Input/Output Diagnostics** link in the list of **Maintenance** tools, the **Core Input/Output Diagnostics** web page opens, as shown in [Figure 19 on page 62](#).

On a Small System, this web page is used to obtain the status of PPP and Ethernet links. The commands available from this web page correspond to the tools traditionally maintained using LD 137 - Core Input/Output Diagnostics.

**Figure 19**  
**Core Input/Output Diagnostics web page - Small System**



To perform diagnostic activities using this web page:

- 1 Select STAT - Status of PPP and ethernet link from the drop-down list.
- 2 Click the **Submit** button.

On a Large System, this web page includes additional commands, as shown in [Figure 20 on page 63](#).

**Figure 20**  
**Core Input/Output Diagnostics web page - Large System**

Managing: **192.167.100.3**  
 System > [Maintenance](#) > Core Input/Output Diagnostics

---

### Core Input/Output Diagnostics

Diagnostic Commands	Command Parameters	Act
STAT - Status of both IOPs and CMDUs and ethernet link	(none) <input type="checkbox"/> ELNK	Sub
TEST CMDU - Test the specified CMDU	(core# slot# device#)	Sub
IDC - Print IDs of both CMDUs and active IOP	(none)	Sub

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

Use the first drop-down list to perform the following diagnostic activities:

- a STAT - Status of both IOPs and CMDUs and ethernet link
- b STAT CMDU - Status of the specified CMDU
- c STAT RDUN - Status of both disks

Use the second drop-down list to perform the following diagnostic activities:

- a TEST CMDU - Test the specified CMDU
- b DATA RDUN - Sector level check on both hard disks
- c TEST RDUN - Test file level check on both hard disks

Use the third drop-down list to perform the following diagnostic activities:

- a IDC - Print IDs of both CMDUs and active IOP
- b IDC CMDU - Print ID for the specified CMDU
- c SDID - Display security device information

## D-channel Diagnostics

Click the **D-channel Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **D-Channel Diagnostics** web page, as shown in [Figure 21](#).

**Figure 21**  
D-channel Diagnostics web page

Managing: 192.167.100.3  
System > Maintenance > D-Channel Diagnostics

### D-Channel Diagnostics

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		Submit
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	Submit
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	Submit
Test Interrupt Generation (TEST 100)		Submit
Establish D-Channel (EST DCH)		Submit

DCH
  DES
  APPL\_STATUS
  LINK\_STATUS
  AUTO\_REC
  PDCH
  BDCH

000   
  DSBL   
  RST   
  AUTO

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

Cancel

This web page is used to test and maintain D-channel links and D-channel Interface (DCHI) cards. The commands available from this web page

correspond to the D-channel data traditionally maintained using the following overlays:

- LD 37 - Input/Output Diagnostic
- LD 48 - Link Diagnostic
- LD 96 - D-channel Diagnostic

To use the diagnostic commands on this web site, do the following:

To execute status commands using this web page, do the following:

- 1** Select one of the following commands from the first **Commands** drop-down list:
  - a** Status for D-Channel (STAT DCH)
  - b** Status for Service Message (STAT SERV)
- 2** Click the **Submit** button.

To execute disable commands using this web page, do the following:

- 1** Select one of the following commands from the second **Commands** drop-down list:
  - a** Disable Automatic Recovery (DIS AUTO)
  - b** Disable D-Channel (DIS DCH). Select the ALL check box to disable all D-Channels.
  - c** Disable Local Loop Back (DIS LLB)
  - d** Disable Remote Loop Back (DIS RLB)
  - e** Disable Test Mode (DIS TEST)
- 2** Click the **Submit** button.

To execute enable commands using this web page, do the following:

- 1** Select one of the following commands from the third **Commands** drop-down list:
  - a** Enable Automatic Recovery (ENL AUTO)
  - b** Enable D-Channel (ENL DCH). To force a loadware download at the same time, click the FDL check box.

- c Enable Local Loop Back (ENL LLB)
- d Enable Remote Loop Back (ENL RLB)
- e Enable Test Mode (ENL TEST)

2 Click the **Submit** button.

To execute test commands using this web page, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a Test interrupt Generation (TEST 100)
  - b Test Loop Back (Test 101)
  - c Test Interrupt Handler (TEST 200)
  - d Test Interrupt Handler-to-link (TEST 201)

2 Click the **Submit** button.

To execute D-Channel commands using this web page, do the following:

- 1 Select one of the following commands from the fifth **Commands** drop-down list:
  - a Establish D-Channel (EST DCH)
  - b Get Physical Address and switch settings (MAP DCH)
  - c Reset DCH and Inhibit Signaling (RST DCH)
  - d Release D-Channel (RLS DCH)
  - e Switch to Standby D-Channel (SDCH DCH)

2 Click the **Submit** button.

## D-Channel Expansion Diagnostics

Click the **D-Channel Expansion Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Link: D-Channel Expansion Diagnostics** web page, as shown in [Figure 22 on page 67](#).

**Figure 22**  
**Link: D-Channel Expansion Diagnostics web page**

Managing: [207.179.153.99](#)  
 System » Maintenance » Link: D-Channel Expansion Diagnostics

---

**Link: D-Channel Expansion Diagnostics**

Diagnostic Commands	Command Parameters	Action
STAT MSDL - Status of MSDL card	(none)	<input type="button" value="Submit"/>
DIS MSDL - Disable the given MSDL card	(none)	<input type="button" value="Submit"/>
ENL MSDL - Enable the given MSDL card	(none)	<input type="button" value="Submit"/>

**MSDL STATUS**  
 No MSDL devices are configured in the system

---

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

This web page is used to test and maintain Multipurpose Serial Data Link (MSDL) cards. The commands available from this web page correspond to the MSDL data traditionally configured using LD 48 - Link Diagnostic.

To perform MSDL diagnostic activities using this web page, do the following.

- 1** Select one of the following commands from the first **Commands** drop-down list:
  - a** STAT MSDL - Status of MSDL card
  - b** STAT MSDL full - Status MSDL card and available RAM
  - c** SLFT MSDL - Self test on the given MSDL card
  - d** RST MSDL - Power-On rest the given MSDL card
- 2** Click the **Submit** button.

To execute disable commands using this web page, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a DIS MSDL all - Disable the given MSDL card
  - b DIS MSDL ALL - Disable all ports and then the MSDL card
  - c DIS MSDL AUDM - Disable MSDL auditing for the MSDL card
  - d DIS MSDL DBG - Disable debugger option for the MSDL card
- 2 Click the **Submit** button.

To execute enable commands using this web page, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a ENL MSDL - Enable the given MSDL card
  - b ENL MSDL all - Enable all ports and then the MSDL card
  - c ENL MSDL AUDM - Enable MSDL auditing for the MSDL card
  - d ENL MSDL FDL - Force download loadware to the MSDL card
- 2 Click the **Submit** button.

## Digital Trunk Diagnostics

The commands available on the **Digital Trunk Diagnostics** web page vary depending on whether the user is working with a Large System or a Small System.

On a Small System, click the **Digital Trunk Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Digital Trunk Interface and Primary Rate Interface: Digital Trunk Diagnostics** web page, as shown in [Figure 23 on page 69](#).

**Figure 23**  
**Digital Trunk Interface and Primary Rate Interface: Digital Trunk Diagnostics web page**

Managing: **192.167.100.3**  
 System > Maintenance > Digital Trunk Interface and Primary Rate Interface :Digital Trunk Diagnostics

---

**Digital Trunk Interface and Primary Rate Interface :Digital Trunk Diagnostics**

Diagnostic Commands	Command Parameters	Action
STAT - Get Status of loop(s)	<input type="text"/> (loop#)	Submit
STAT - Get Status of the Channel	<input type="text"/> (# ch#)	Submit
LOVF - List Threshold Overflows for Route	<input type="text"/> (cust# route#)	Submit
ATLP - Daily routine auto loop test	<input type="text"/> (0 or 1)	Submit

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

This web page is used to test and maintain Digital Trunk Cards. The commands available from this web page correspond to the DTI/PRI data traditionally maintained using LD 60 - Digital Trunk Interface and Primary Rate Interface Diagnostics.

Use this web page to issue maintenance commands on cards, channels, or routes using the appropriate command drop-down list and parameter text box.

To perform maintenance activities on a Digital Trunk Card on a Small System using this web page, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT - Get Status of the Card(s)
  - b DISL - Disable the card
  - c DISI - Disable the card (when all channels are idle)

- d** ENCH - Enable all channels on the card
- e** ENLL - Enable the Card
- f** LCNT - List contents of Alarm Counters on Card(s)
- g** RCNT - Reset Alarm Counters on Card(s)
- h** SLFT - Self Test on the card
- i** DSYL - Disable Yellow Alarm Processing on the card
- j** ENYL - Enable Yellow Alarm Processing on the card
- k** DLBK - Disable remote loop back test
- l** RLBK - Perform external loop back test on card
- m** RMST - Perform a far end loop test on card

- 2** Enter the Card number in the **Command Parameters** text box.
- 3** Click the **Submit** button.

To perform maintenance activities on a Channel belonging to a Digital Trunk Card on a Small System using this web page, do the following:

- 1** Select one of the following commands from the second Commands drop-down list:
  - a** STAT - Get Status of the channel
  - b** DSCH - Disable the channel
  - c** ENCH - Enable the channel
  - d** SLFT - Self Test on the channel
  - e** DLBK - Disable remote loop back test on channel
  - f** RLBK - Perform external loop back test on channel
  - g** RMST - Perform far end loop test on channel
  - h** RSET - Reset thresholds for channel.
- 2** Enter the Card number and the Channel number, separated by a space, in the **Command Parameters** text box.
- 3** Click the **Submit** button.

To perform maintenance activities on a Digital Trunk Route on a Small System using this web page:

- 1 Select the command from the third **Commands** drop-down list:
  - a LOVF - List Thresholds Overflows for the Route
  - b CMIN - Clear minor alarm indication for cust
- 2 Enter the Customer number and the Route number, separated by a space, in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To perform maintenance activities on a card on a Small System using this web page:

- 1 Select the command from the fourth **Commands** drop-down list:
  - a ATLP - Daily routine automatic card test
  - b CMIN ALL - Clear minor alarm indication
  - c CDSP - Clear maintenance display
- 2 Enter the 0 or 1 in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute loop commands on a Large System using this web page, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT - Get status of loop (s)
  - b DISL - Disable network and DTI/PRI cards of loop
  - c DISI - Disable loop (when all channels are idle)
  - d ENCH - Enable all channels on a 20 Mb/s DTI/PRI
  - e ENLL - Enable network and DTI/PRI cards of loop
  - f LCNT - List contents of alarm counters on loop(s)
  - g RCNT - Reset alarm counters of all DTI/PRI loops

- h** SLFT - Self Test on the loop
- i** DSYL - Disable yellow alarm processing for loop
- j** ENYL - Enable yellow alarm processing for loop
- k** DLBK - Disable remote loop back test
- l** RLBK - Close loop at carrier interface point for testing
- m** RMST - Perform remote loop back test on loop

- 2** Enter the loop number in the **Command Parameters** text box.
- 3** Click the **Submit** button.

## Digital Trunk Maintenance Diagnostics

Click the **Digital Trunk Maintenance Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Digital Trunk Diagnostics** web page, as shown in [Figure 24](#).

**Figure 24**  
Digital Trunk Diagnostics web page

Managing: 192.167.100.3  
System » Maintenance » Digital Trunk Diagnostics

### Digital Trunk Diagnostics

Diagnostic Commands	Command Parameters	Action
STAT DDCS - Status for All DDCS loops or loop	<input type="text"/> ((loop))	<input type="button" value="Submit"/>
DIS DDCS - Disable DDCS number	<input type="text"/> (number)	<input type="button" value="Submit"/>
ENL DDCS - Enable DDCS number	<input type="text"/> (number)	<input type="button" value="Submit"/>
CDSP - Clear Display on active CPU	<input type="text"/> (none)	<input type="button" value="Submit"/>

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

The commands available from this web page correspond to the digital trunk diagnostics traditionally performed using LD 60 - Digital Trunk Interface and Primary Rate Interface.

To get status information on a digital trunk using this web page, do the following:

- 1 Select one of the following status commands from the first **Commands** drop-down list:
  - a STAT DDCS - Status for all DDCS loops or loop
  - b STAT DDSL - Status for all DDSLs or DDSL number

- c STAT DTCS - Status for all DTCS loops or DTCS loop
- d STAT DTRC - Status of RDC on loop
- e STAT DTSL - Status of all DTSLs or DTSL number
- f STAT DTVC - Status of VDC on loop
- g STAT LSSL - Status of LSSL number for APNSS
- h STAT LSRC - Status of RDC on Signaling Link number
- i STAT LSVC - Status of VDC on Signaling Link number

- 2 Enter the Loop number in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To disable an entity on a digital trunk using this web page, do the following:

- 1 Select one of the following disable commands from the second **Commands** drop-down list:
  - a DIS DDSC - Disable DDSC number
  - b DIS DDSL - Disable DDSL number
  - c DIS DTCS - Disable DTCS loop
  - d DIS DTRC - Disable RDC on Loop
  - e DIS DTSL - Disable DTSL number
  - f DIS DTVC - Disable VDC on loop
  - g DIS LSSL - Disable LSSL number for APNSS
  - h DISI DDSC - Disable all Channels on Loop as idle
  - i DISI DTCS - Disable DTCS loop
- 2 Enter the appropriate number in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To enable an entity on a digital trunk using this web page, do the following:

- 1 Select one of the following enable commands from the third **Commands** drop-down list:
  - a ENL DDSC - Enable DDSC number
  - b ENL DDSL - Enable DDSL number
  - c ENL DTCS - Enable DTCS loop
  - d ENL DTRC - Enable RDC on Loop
  - e ENL DTSL - Enable DTSL number
  - f ENL DTVC - Enable VDC on loop
  - g ENL LSSL - Enable LSSL number for APNSS
- 2 Enter the appropriate number in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To perform miscellaneous commands on a digital trunk using this web page, do the following:

- 1 Select one of the following enable commands from the fourth **Commands** drop-down list:
  - a CDSP - Clear display on active CPU
  - b CMIN ALL - Reset Alarm Indication For All Customers
  - c CMIN - Reset Alarm Indication for Customer
  - d STRT - Start DDSL number
- 2 Click the **Submit** button.

## Ethernet Diagnostics

Click the **Ethernet Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Ethernet Diagnostics** web page, as shown in [Figure 25 on page 76](#).

**Figure 25**  
**Ethernet Diagnostics web page**

Managing: **192.167.100.3**  
 System > Maintenance > Ethernet Diagnostics

---

### Ethernet Diagnostics

Status Commands [ -- Filters ]	Command Parameters
STAT LINK IP - Link status -- IP	<input type="text"/> <input type="button" value="Submit"/>
STAT SERV - Server status	<input type="text"/> <input type="button" value="Submit"/>
STIP TN - IP Status -- TN	<input type="text"/> <input type="button" value="Submit"/>
PRT IPDN - Print DNS with a given IP address	<input type="text"/> <input type="button" value="Submit"/>
ECNT FW - Etherset Count -- FWID MajorVer MinorVer Filter	<input type="text"/> <input type="button" value="Submit"/>
RST ZONE - Reset IP Phone -- Zone START/STOP HH:MM	<input type="text"/> <input type="button" value="Submit"/>

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

This web page is used to maintain Ethernet elements. The commands available from this web page correspond to the data traditionally maintained using LD 117- Ethernet Quality of Service Diagnostics.

To execute Link status commands, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT LINK IP - Link Status -- IP
  - b STAT LINK SRV - Link Status -- Server
  - c STAT LINK NAME - Link Status -- Host Name
  - d STAT LINK NODE - Link Status -- Node ID

- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute server status commands, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a STAT SERV - Server Status
  - b STAT SERV IP - Server Status -- IP
  - c STAT SERV TYPE - Server Status -- Type
  - d STAT SERV APP - Server Status -- Application
  - e STAT SERV NAME - Server Status -- Name
  - f STAT SERV NODE - Server Status -- Node ID
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute IP status commands, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a STIP TN - IP Status -- TN
  - b STIP TYPE - IP Status -- Type
  - c STIP ZONE - IP Status -- Zone
  - d STIP NODE - IP Status -- Node ID
  - e STIP HOSTIP - IP Status -- Host IP
  - f STIP ACF - IP Status -- Active Call Failover
  - g STIP TERMIP - IP Status -- Term IP
  - h STIP FW - IP Status -- FWID MajorVer MinorVer Filter

i STIP MODL - IP Status -- ModelName

- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute print commands, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a PRT IPDN - Print DNs with a given IP address
  - b PRT DNIP Print IP address(es) with a given DN
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute Etherset Count commands, do the following:

- 1 Select one of the following commands from the fifth **Commands** drop-down list:
  - a ECNT FW - Etherset Count -- FWID MajorVer MinorVer Filter
  - b ECNT MODL - Etherset Count -- Model
  - c ECNT PEC - Etherset Count -- PEC
  - d ECNT ZONE - Etherset Count -- Zone Customer #
  - e ECNT CARD - Etherset Count -- Loop Shelf Card Customer#
  - f ECNT NODE - Etherset Count -- Node ID
  - g ECNT SS - Etherset Count -- HostName
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute Reset IP Phone commands, do the following:

- 1 Select one of the following commands from the sixth **Commands** drop-down list:
  - a RST ZONE - Reset IP Phone -- Zone START/STOP HH:MM
  - b RST FW - Reset IP Phone -- FWID START/STOP HH:MM
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

## Ethernet Quality of Service Diagnostics

Click the **Ethernet Quality of Service Diagnostic** link in the list of **Maintenance** diagnostic tools to open the **Ethernet Quality of Service Diagnostics** web page, as shown in [Figure 26 on page 80](#).

**Figure 26**  
**Ethernet Quality of Service Diagnostics web page**

Managing: 207.179.153.99  
System » Maintenance » Ethernet Quality Of Service Diagnostics

### Ethernet Quality Of Service Diagnostics

Action:  Zone Number:  Attribute:

Action:  Zone Number:  Level:

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

This web page is used to issue commands on elements by using the appropriate **Action** drop-down list and the corresponding Zone Number and Attribute or Level text boxes.

The commands available from this web page correspond to data traditionally maintained using LD 117 - Zone Configuration and Diagnostic.

To perform maintenance activities for Zone Attributes:

- 1 Select one of the following commands from the **Action** drop-down list:
  - a Print QoS attribute for Zone (PRT AQOS)
  - b Print Zone IP statistics (PRT ZQOS)
- 2 Enter the appropriate value in the corresponding **Zone Number** and **Attribute** text box.
- 3 Click **Submit**.

To perform maintenance activities for Zone Levels:

- 1 Select one of the following commands from the **Action** drop-down list:
  - a Change Zone Notification Level (CHG ZQNL)
  - b Print Zone Notification Level (PRT ZQNL)
- 2 Enter the appropriate value in the corresponding **Zone Number** and **Level** text box.
- 3 Click the **Submit** button.

## Event Preference Table (EPT)

Click the **Event Preference Table** link in the list of **Maintenance** tools to open the **Event Preference Table (EPT)** web page, as shown in [Figure 27](#).

**Figure 27**  
**Event Preference Table (EPT) web page**

Managing: 207.179.153.99  
System > Maintenance > Event Preference Table (EPT)

### Event Preference Table (EPT)

Select the file

Export the Active EPT file

Display the Active EPT file

This web page is used to import and export selected SNMP Event Preference Tables. When alarms are generated, the EPT specifies which alarms should or should not be sent to the SNMP agent. It can also display the active EPT for the Call Server.

The EPT files are stored on the Call Server. Alarm throttling specifies how many alarms can be sent within a given interval, and is determined by the EPT file. The EPT files can be edited with any text editor.

## Input/Output Diagnostics

Click the **Input/Output Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Input Output Diagnostics** web page, as shown in [Figure 28](#).

**Figure 28**  
**Input/Output Diagnostics web page**

Managing: 192.167.100.3  
System > Maintenance > Input Output Diagnostics

### Input Output Diagnostics

Diagnostic Commands	Command Parameters	Action
----- TTY Commands -----	<input type="text"/>	Submit
----- Printer Commands -----	<input type="text"/>	Submit
----- MSDL Commands -----	<input type="text"/>	Submit
----- Miscellaneous Commands -----	<input type="text"/>	Submit

**MSDL STATUS**  
No MSDL devices are configured in the system

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

The commands available from this web page correspond to the Input Output diagnostics traditionally performed using LD 37 - Input/Output.

To execute TTY commands, do the following.

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT TTY - Get status of TTY device(s)
  - b ENL TTY - Enable TTY
  - c DIS TTY - Disable TTY
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute Printer commands, do the following.

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a STAT PRT - Get status of Printer(s)
  - b ENL PRT - Enable Printer
  - c DIS PRT - Disable Printer
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To execute MDSL commands, do the following.

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a STAT MSDL - Get status of MSDL card(s)
  - b ENL MSDL - Enable MSDL device
  - c DIS MSDL - Disable MSDL device
  - d SLFT MSDL - Self test MSDL device
  - e RST MSDL - Reset MSDL device

- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the miscellaneous commands, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a STAT - Get status of all I/O devices in system
  - b STAT XSM - Get status of the system monitor
  - c STAT LINK - Get status of CDR data Link(s)
  - d CMIN - Clear minor lamp on system basis
  - e CMIN ALL - Clear minor alarm on all attendant consoles
  - f CDSP - Clear maintenance display on active CPU
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

## Intergroup Switch and System Clock Generator Diagnostics

The **Intergroup Switch and System Clock Generator Diagnostics** web page is available only on Large Systems.

Click the **Intergroup Switch and System Clock Generator Diagnostics** link in the list of **Call Server** functionalities to open the **Intergroup Switch and System Clock Generator Diagnostics** web page, as shown in [Figure 29](#).

**Figure 29**  
**Intergroup Switch and System Clock Generator Diagnostics web page**

Managing: **192.167.100.3**  
System > Maintenance > Intergroup Switch and System Clock Generator Diagnostics

---

### Intergroup Switch and System Clock Generator Diagnostics

Diagnostic Commands	Command Parameters	Action
STAT FIJI - Status of FIJI in specified Grp, Side	<input type="text"/> (grp# side#)	<input type="button" value="Submit"/>
DIS ALRM - Disable specified Alarm (or all) for FIJI	<input type="text"/> (grp# side# (alarm#))	<input type="button" value="Submit"/>
ENL ALRM - Enable specified Alarm (or all) for FIJI	<input type="text"/> (grp# side# (alarm#))	<input type="button" value="Submit"/>
TEST 360 - Perform 360 test on FIJI card	<input type="text"/> (grp# side# (time#))	<input type="button" value="Submit"/>
CDSP - Clear Maintenance Display on active CPU	<input type="text"/> (none)	<input type="button" value="Submit"/>

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

The commands available from this web page correspond to the Intergroup Switch and System Clock Generator diagnostics traditionally performed using LD 39.

To use status miscellaneous commands, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT FIJI - Status of FIJI on specified Grp, Side
  - b STAT IGS - Status of specified IGS card(0-19)
  - c STAT PER - Status of specified PS card
  - d STAT SCG - Status of specified SCG card(0 or 1)
  - e STAT RING - Status of all FIJI cards on specified Ring
- 2 Enter the group number and side number in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the disable commands, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a DIS ALRM - Disable specified Alarm (or all) for FIJI
  - b DIS FIJI - Disable FIJI in specified Group and Side
  - c DIS IGS - Disable specified IGS card(0-19)
  - d DIS IGS - Disable specified IGS card when idle
  - e DSPS - Disable specified PS card
  - f DIS SCG - Disable specified SCG card(0 or 1)
  - g DIS RING - Disable all FIJI cards on specified Ring
  - h DIS RALM - Disable all alarms for all RIJI cards in Ring
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the enable commands, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a ENL ALRM - Enable specified Alarm (or all) for FIJI
  - b ENL FIJI - Enable FIJI in specified Group and Side
  - c ENL IGS - Enable specified IGS card(0-19)
  - d ENPS - Enable specified PS card
  - e ENL SCG - Enable specified SCG card(0 or 1)
  - f ENL RING - Enable all FIJI cards on specified Ring
  - g ENL RALM - Enable all alarms for all FIJI cards in Ring
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the test commands, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a TEST 360 - Perform 360 test on FIJI card
  - b TEST FIJI - Self Test FIJI Card
  - c TEST BKPL - Test backplane
  - d TEST CMEM - Test connection memory
  - e TEST LINK - Perform Link test to identify hardware faults
  - f TEST ALL - Perform FIJI diagnostic test
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the miscellaneous commands, do the following:

- 1 Select one of the following commands from the fifth **Commands** drop-down list:
  - a CDSP - Clear Maintenance Display on active CPU
  - b CMIN - Clear minor alarm on attendant console
  - c CMIN ALL - Reset minor alarm on attendant consoles
  - d ARCV ON - Set auto-recovery operation for ring
  - e ARCV OFF - Reset auto-recovery operation for ring
  - f ALRD ON - Turn on alarm display for all FIJI cards
  - g ALRD OFF - Turn off alarm display for all FIJI cards
  - h RSET - Reset thresholds for switchover functionality
  - i RSTR - Restore Ring(s)
  - j SCLK - Switchover to the other SCG
  - k SLCK FRCE - Force clock to switch to other SCG
  - l SWRG - Switch Call Processing to specified ring
- 2 Click the **Submit** button.

## MSDL Diagnostics

Click the **MSDL Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Multipurpose Serial Data Link (MSDL) Diagnostics** web page, as shown in [Figure 30](#).

**Figure 30**  
**MSDL Diagnostics web page**

Managing: [192.167.100.3](#)  
System > [Maintenance](#) > MSDL Diagnostics

### MSDL Diagnostics

Diagnostic Commands	Command Parameters	Action
<input type="text" value="Disable MSDL Device (DIS)"/>	<input type="checkbox"/> FDL <input checked="" type="checkbox"/> FULL <input type="checkbox"/> ALL	<input type="button" value="Submit"/>

**MSDL STATUS**  
No MSDL devices are configured in the system

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

The commands available from this web page correspond to the MSDL diagnostics traditionally performed using LD 96 - D-channel.

This web page is used to perform the following MSDL diagnostic functions:

- Disable MSDL Device (DIS)
- Enable MSDL Device (ENL)
- Self Test (SLFT)
- Get Status of MSDL Device (STAT)
- Causes Power-On Reset of MSDL Device (RST)

To perform diagnostic activities using this web page:

- 1 Select the required **Diagnostic Command** from the drop-down list.
- 2 To update the loadware, select the **FDL (Force Download)** check box when the Enable MSDL Device command is selected. To check the status of all MDSL devices, select the **Full** check box when the Get Status of MSDL Device command is selected.
- 3 Enter any required **Command Parameters**. The required parameters for the selected command are indicated to the right of the **Command Parameters** box once the command is selected.
- 4 Click the **Submit** button.

## Multifrequency Sender Diagnostics

The **Multifrequency Sender Diagnostics** web page is available only on Large Systems.

Click the **Multifrequency Sender Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Multifrequency Sender Diagnostics** web page, as shown in [Figure 31](#).

**Figure 31**  
**Multifrequency Sender Diagnostics web page**

Managing: [192.167.100.3](#)  
System » [Maintenance](#) » Multifrequency Sender Diagnostics

---

### Multifrequency Sender Diagnostics

Diagnostic Commands	Command Parameters	Action
----- Loop Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Card Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Alarm Commands -----	<input type="text"/>	<input type="button" value="Submit"/>

---

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

The commands available from this web page correspond to the Multifrequency Sender diagnostics traditionally performed using LD 46.

To use the loop commands, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT - GetStatus of MFS loop
  - b ENLL - Enable loop
  - c DISL - Disable loop
  - d MFS - Test and enable MFS loop
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the card commands, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a ENLX - Enable Conf/TDS/MFS card on loop
  - b DISX - Disable Conf/TDS/MFS card on loop
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the alarm commands, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a CMAJ - Clear major alarm and reset power fail
  - b CDSP - Clear Maint display on active CPU
  - c CMIN - Clear minor lamp on system
  - d CMIN ALL - Clear minor lamp on atndt consls
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

## Multifrequency Signaling Diagnostics

Click the **Multifrequency Signaling Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Multifrequency Signaling Diagnostics** web page, as shown in [Figure 32](#).

**Figure 32**  
Multifrequency Signaling Diagnostics web page

Managing: [192.167.100.3](#)  
System > [Maintenance](#) > Multifrequency Signaling Diagnostics

### Multifrequency Signaling Diagnostics

Diagnostic Commands	Command Parameters	Action
----- Card Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Unit Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Miscellaneous Commands -----	<input type="text"/>	<input type="button" value="Submit"/>

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

The commands available from this web page correspond to the Multifrequency Signaling diagnostics traditionally performed using LD 54 - Multifrequency Signaling.

To use the card commands, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT - Get status of MFC or MFE card
  - b DISC - Disable XMFC/XMFE card

- c ENLC - Enable MFC or MFE card
  - d MIDN - Reset/Initialize all idle MFC or MFE cards
- 2 Enter the required command parameters in the **Command Parameters** text box.
  - 3 Click the **Submit** button.

To use the unit commands, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a STAT - Get status of specified MFC or MFE unit
  - b DISU - Disable XMFC/XMFE channel
  - c ENLU - Enable XMFC/XMFE channel
  - d MTST - Invoke loop around test on unit with digit and level
  - e ATST - Invoke automatic loop test for unit
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the miscellaneous commands, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a STAT - List all disabled XMFC/XMFE channels in system
  - b CMIN - List all disabled MFC channels in the system (Large System only)
  - c CMIN ALL - Clear minor alarm on all attendant consoles (Large System only)
  - d CDSP - Clear the mtc display on active CPU (Large System only)
  - e CMAJ - Clear major alarm and reset power fail transfer (Large System only)

- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

## Network and Peripheral Equipment Diagnostics

Click the **Network and Peripheral Equipment Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Network & Peripheral Diagnostics** web page, as shown in [Figure 33](#).

**Figure 33**  
**Network & Peripheral Diagnostics web page**

Managing: **192.167.100.3**  
System » [Maintenance](#) » Network & Peripheral Diagnostics

### Network & Peripheral Diagnostics

Diagnostic Commands	Command Parameters	Action
----- Loop Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- Shelf Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- Card Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- Unit Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- M39XX Unit Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- BRI SILC/UILC Commands ----	<input type="text"/>	<input type="button" value="Submit"/>

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

This web page is used to test and maintain network and peripheral equipment. The commands available from this web page correspond to the data traditionally maintained using the LD 32 - Network and Peripheral Equipment Diagnostic.

These commands are split among separate drop-down lists, grouped by equipment type. On a Large System, there are six drop-down lists; on a Small System there are five. Some commands act on different system components, depending on whether they are being executed on a Large or Small System.

The command lists are as follows:

- Loop Commands (Large System only)
  - Network Loop
    - ENLL - Enable network loop
    - DISL - Disable network loop
  - Super Loop
    - STAT - Get status of Superloop
    - SUPL - Print data for one or all Superloops
    - IDC - Print Card ID for Superloop and associated Controller
    - XNTT - Do self-test of Network card for specified Superloop
    - ENLL - Enable specified Superloop
    - XRST - Reset the specified Superloop
- Shelf Commands
  - DISS - Disable module (Small System) Disable the shelf (Large System)
  - ENLS - Enable module (Small System) Enable specified shelf (Large System)
  - LBSY - List TNs of all busy units
  - LDIS - List TNs of all disabled units
  - LIDL - List TNs of all idle units
  - LMNT - List TNs of all maint. busy units
- Card Commands
  - General Card Commands
    - STAT - Get card status

- ENLC - Enable and reset card
- DISC - Disable card (Small System). Disable peripheral card (Large System)
- IDC - Print card ID (Small System). Print card ID for PE card (Large System)
  
- MISP Card Commands
  - STAT - Print status of MISP appl/card
  - ENCL - Enable MISP card (Small System)
  - ENLL - Enable MISL loop (Large System)
  - ENLC BRIL - Enable BRIL application on MISP (Small System)
  - ENLL BRIL - Enable BRIL application on MISP loop (Large System)
  - ENLC BRIT - Enable BRIT application on MISP (Small System)
  - ENLL BRIT - Enable BRIT application on MISP loop (Large System)
  - IDC - Print MISP card ID
  - DISC - Disable MISP card (Small System)
  - DISL - Disable MISP loop (Large System)
  - DISL BRIL - Disable BRIL application on MISP (Small System)
  - DISL BRIL - Disable BRIL application on MISP loop (Large System)
  - DISC BRIT - Disable BRIT application on MISP (Small System)
  - DISL BRIT - Disable BRIT application on MISP loop (Large System)

- DISC BRIE - Disable BRIE application on MISP (Small System)
- DISL BRIE - Disable BRIE application on MISP loop (Large System)
- BRI BRSC Card Commands
  - STAT - Get status of BRI card
  - IDC - Print BRSC card and LW version
  - DISC BRI - Disable the BRSC BRI application
  - DISC - Disable specified card
  - ENLC BRI - Enable the BRSC BRI application
  - ENLC - Enable specified card
- PS Card Commands (Large System)
  - STAT PER - Get status of PS card
  - ENPS - Enable PS card and associated loops
  - DSPS - Disable Peripheral Signaling card
- Network Card Commands (Large System)
  - STAT NWK - Check status of N/W card with specified loop
  - ENLN - Enable network card with specified loop
  - DISN - Disable network card with specified loop
- XPEC Controller Commands (Large System)
  - XPEC - Print data for all or specified Controller(s)
  - ENXP - Enable Controller and associated cards
  - ENXP XPC - Enable Controller, not the associated cards
  - DSXP - Disable Controller and all connected cards
  - XPCT - Self-test on Controller
  - IDCs - Print card ID for cards

- Unit Commands
  - General Unit Commands
    - STAT - Get unit status
    - ENLU - Enable unit
    - IDU - Print set ID
    - DISU - Disable unit
    - STAT VTRM - Display virtual trunk unit status
- M39XX Unit Commands
  - FDLN - Cancel/stop flash download for M39xx
  - FDLU - Conditional download to one M39xx
  - FWVU - Print firmware versions on M39xx
  - FSUM - Print firmware versions on M39xx
- BRI SILC/UILC Commands
  - STAT - Get status of SILC or UILC
  - ENL AUTO - Enable automatic link recovery
  - ENRB - Enable Remote Loop Back for DSL
  - DIS AUTO - Disable automatic link recovery
  - DISU - Disable the DSL
  - DSRB - Disable Remote Loop Back for DSL
  - IDC - Print SILC/UILC card ID
  - PERR - Print protocol log for the card
  - DISC - Disable SILC/UILC card
  - FDIS NCAL - Force disconnect the connection
  - STAT NCAL - List all current connections - DSL

Use this web page to issue diagnostic commands on the network and peripheral equipment by using the appropriate **Diagnostic Commands** drop-down list and the corresponding **Command Parameters** text box. The required parameters for the selected command are indicated to the right of the **Command Parameters** box once the command is selected.

To perform maintenance activities using this web page:

- 1 Select a command from one of the **Diagnostic Commands** drop-down lists.
- 2 Enter the appropriate value in the corresponding **Command Parameters** text box. The required parameters for the selected command are indicated to the right of the **Command Parameters** box once the command is selected.
- 3 Click the corresponding **Submit** button.

## Network and Signaling Diagnostics

Click the **Network and Signaling Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Network & Signaling Diagnostics** web page, as shown in [Figure 34](#).

**Figure 34**  
**Network & Signaling Diagnostics web page**

Managing: [192.167.100.3](#)  
System > Maintenance > Network & Signaling Diagnostics

### Network & Signaling Diagnostics

Diagnostic Commands	Command Parameters	Action
----- Loop Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Shelf/Card/Unit Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- BRI Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Superloop Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Alarm Commands -----	<input type="text"/>	<input type="button" value="Submit"/>

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

The commands available from this web page correspond to the Network and Signaling diagnostics traditionally performed using LD 30 - Network and Signaling.

This web page is used to perform the following Network and Signaling diagnostic functions:

- Loop Commands (Large System only)
  - ENLL - Enable network loop
  - DISL - Disable loop
  - LDIS - List disabled loops

- LENL - List enabled loops
- LOOP - Test network memory on loop(s)
- STAT - Get status of all/specified N/W loops
- TTSM - Test TSM of a loop
- Shelf/Card/Unit Commands
  - TEST - Continuity and signaling test on XPE (Small System)
  - UNTT - Signaling test on specified card or unit
  - SHLF - Test loop l, shelf s (Large System)
  - CPED - Clear contents of ctrlr maint display (Large System)
  - RPED - Read contents of ctrlr maint display (Large System)
  - TTWI - Test TSM of the N/W card (Large System)
- BRI Commands
  - SLFT - Selftest on ISDN BRI line card
  - SLFT - Selftest ISDN BRI line card (Large System)
  - SLFT - Selftest on MISP card
  - STEI - Query Term Edpt Identifiers and USIDs (Large System)
  - TEIT - Perform TEI check on DSL
- Superloop Commands (Large System)
  - ENLL - Enable specified Superloop
  - DISL - Disable specified Superloop
  - ENLL - Enable sl, download periph s/w ver
- Alarm Commands
  - CMAJ - Clear major alarm and reset power fail
  - CDSP - Clear Maint display on active CPU
  - CMIN - Clear minor alarm on attendant consoles for customer
  - CMIN ALL - Clear minor alarm on all attendant consoles

To perform diagnostic activities using this web page:

- 1 Select the required **Diagnostic Command** from the drop-down list.
- 2 Enter any required **Command Parameters**. The required parameters for the selected command are indicated to the right of the **Command Parameters** box once the command is selected.
- 3 Click the **Submit** button.

## TMDI Diagnostics

T1 Multipurpose Digital Interface (TMDI) cards are used only in CS 1000M Small Systems. Click the **TMDI Diagnostics** link in the list of **Call Server** diagnostic tools to open the **TMDI Diagnostics** web page, as shown in [Figure 35 on page 103](#).

**Figure 35**  
**TMDI Diagnostics web page**

Managing: 207.179.153.99  
System > Maintenance > TMDI Diagnostics

### TMDI Diagnostics

Diagnostic Commands	Command Parameters	Action
Enable TMDI Card (ENL) ▾	<input type="checkbox"/> FDL <input type="checkbox"/> FULL <input type="checkbox"/> ALL	<input type="button" value="Submit"/>

TMDI STATUS

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

This web page is used to test and maintain TMDI (DTI/PRI/DCH) cards. The commands available from this web page correspond to the TMDI data traditionally configured using LD 96 - D-channel.

To perform diagnostic activities using this web page:

- 1 Select one of the following **Actions** from the drop-down list:
  - a Enable TMDI Card (ENL)
  - b Disable TMDI card (DIS)
  - c Self Test on TMDI Card (SLFT)
  - d Get TMDI Status (STAT)
- 2 Enter any required **Command Parameters**. The required parameters for the selected command are indicated to the right of the **Command Parameters** box once the command is selected.
- 3 Click the **Submit** button.

## Tone and Digit Switch Diagnostics

Click the **Tone and Digit Switch Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Tone and Digit Switch and Digitone Receiver Diagnostics** web page, as shown in [Figure 36](#).

**Figure 36**

**Tone and Digit Switch and Digitone Receiver Diagnostics web page**

Managing: **192.167.100.3**  
System > Maintenance > Tone and Digit Switch and Digitone Receiver Diagnostics

---

### Tone and Digit Switch and Digitone Receiver Diagnostics

Diagnostic Commands	Command Parameters	Action
----- Loop Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Card and Unit Commands -----	<input type="text"/>	<input type="button" value="Submit"/>
----- Miscellaneous Commands -----	<input type="text"/>	<input type="button" value="Submit"/>

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

The **Tone and Digit Switch and Digitone Receiver Diagnostics** web page has different menus depending on whether it is on a Large or a Small System.

This web page is used to execute tone, digit switch, and digitone receiver diagnostics. The commands available from this web page correspond to the TMDI data traditionally configured using LD 34 - Tone and Digital Switch.

To perform diagnostic activities using this web page:

1 Select one of the following **Diagnostic Commands** from the drop-down lists:

- Loop Commands (Large System)
  - STAT - Get status TDS loop
  - DISL - Disable tone and digit loop
  - DISX - Disable Conf/TDS/MFS card on loop 1 and 1 + 1
  - ENLX - Enable Conf/TDS/MFS card on loop 1 and 1 + 1
  - ENLL - Enable tone and digit loop
  - MFR - Test ANI Feature Group D Multifrequency receiver units
  - TDS - Test outpulsers and channels on loop
- Card and Unit Commands
  - STAT - List TNs of all disabled DTRs and MFRs (Small System)
  - SDTR - Get status of DTR/MFR or XDT card/unit
  - DISX - Disable the TDS/MFS card (Small System)
  - DISR - Disable specified TDS/MFS card/unit
  - ENLX - Enable the TDS/MFS card (Small System)
  - ENLR - Enable the DTR/MFR card/unit
  - DTR - Test specified Digitone receiver card/unit
  - MFR - Test all ANI Multifrequency receiver units
  - TDS - Test outpulsers and channels (Small System)
- Miscellaneous Commands
  - CMIN - Clear the minor alarm on all attendant consoles for customer (Large System)
  - CMIN ALL - Clear minor alarm on all attendant consoles
  - CDSP - Clear the mtc display on active CPU

- CMAJ- Clear major alarm and reset power fail transfer
  - MFR - Test all ANI Feature Group D MFR receiver units
- 2 Enter any required **Command Parameters**. The required parameters for the selected command are indicated to the right of the **Command Parameters** box once the command is selected.
  - 3 Click the corresponding **Submit** button.

## Trunk Diagnostics

Click the **Trunk Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Trunk Diagnostics** web page, as shown in [Figure 37 on page 107](#).

**Figure 37**  
**Trunk Diagnostics web page**

Managing: **192.167.100.3**  
System » Maintenance » Trunk Diagnostics

---

### Trunk Diagnostics

Diagnostic Commands	Command Parameters	Action
----- Card Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- Unit Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- Customer Route Commands ----	<input type="text"/>	<input type="button" value="Submit"/>
----- Miscellaneous Commands ----	<input type="text"/>	<input type="button" value="Submit"/>

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

This web page is used to test and maintain trunk cards. There are different commands available depending on whether the web page is on a Large or a Small System. The commands available from this web page correspond to the data traditionally maintained using LD 36 - Trunk Diagnostic.

To use the card commands, do the following:

- 1 Select one of the following commands from the first **Commands** drop-down list:
  - a STAT - Get card status
  - b ENLC - Enable and reset card
  - c DISC - Disable card
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the unit commands, do the following:

- 1 Select one of the following commands from the second **Commands** drop-down list:
  - a ENLU - Enable unit
  - b LDIC - Number of days since last inc. call (Large System)
  - c DISU - Disable unit
  - d RSET - Reset thresholds for the trunk
  - e TPPM - Test the specified PPM trunk (Large System)
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the customer route commands, do the following:

- 1 Select one of the following commands from the third **Commands** drop-down list:
  - a LDIC - List days since last incoming call for customer
  - b LMAX - List trunk with max idle days for customer
  - c LNDS - List trunks with no disconnect sup. for customer
  - d LOVF - List threshold overflows for customer
  - e RAN - Test recorded announcement device
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

To use the miscellaneous commands, do the following:

- 1 Select one of the following commands from the fourth **Commands** drop-down list:
  - a CMIN - Clear the minor lamp on a system basis (Large System)
  - b CMIN ALL - Clear minor alarm on all attendant consoles
  - c CDSP - Clear the mtc display on active CPU
- 2 Enter the required command parameters in the **Command Parameters** text box.
- 3 Click the **Submit** button.

## Zone Diagnostics

Click the **Zone Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **Maintenance Commands for Zones** web page, as shown in [Figure 38](#).

**Figure 38**  
**Maintenance Commands for Zones web page**

Managing: **192.167.100.3**  
 System » [Maintenance](#) » Maintenance Commands for Zones

---

### Maintenance Commands for Zones

Action

Zone Number

---

Zone Number	State	Resource Type	Intrazone Strategy	Zone Intent	Bandwidth(Kbps)	Usage(Kbps)	Peak(%)
0	ENABLED	SHARED	BQ	MO	10000	0	0

Number of Zones configured = 1

This web page is used to enable and disable zones and to view various parameters, properties, and behaviors associated with the configured zones. The commands available from this web page correspond to the data traditionally maintained using LD 117 - Ethernet and Alarm Management.

This web page also includes a table that shows the status and settings for the configured zones.

To perform maintenance activities using this web page:

- 1 Select one of the following **Actions** from the drop-down list:
  - a Print Intrazone Statistics per Local Zone (PRT INTRAZONE)
  - b Print Bandwidth Property (PRT ZBW)
  - c Print Description (PRT ZDES)
  - d Print Dialing Plan and Access Codes (PRT ZDP)

- e Print Emergency Service Access Information (PRT ZESA)
  - f Print Time Change property (PRT ZTP)
  - g Show Branch Office Behaviour (STAT ZBR)
  - h Show Status (STAT ZONE)
  - i Enable a Zone (ENL ZONE)
  - j Disable a Zone (DIS ZONE)
  - k Enable a Zone's Branch Office Behaviour (ENL ZBR)
  - l Disable a Zone's Branch Office Behaviour (DIS ZBR)
  - m Print Adaptive Network Bandwidth Management and CAC Parameters (PRT ZCAC)
  - n Print Interzone Statistics (PRT INTERZONE)
  - o Reset CAC Statistics (CLR CACR)
  - p Print Zone Alternate Prefix Information (PRT ZALT)
  - q Show Alternate Routing Status (STAT ZALT)
  - r Print Alarm Suppression Time Period (PRT ZAST)
- 2 Enter the Zone Number assigned to a configured zone in the **Zone Number** text box.
  - 3 Click the **Submit** button.

This web page provides peripheral software application data and the corresponding version numbers for peripheral software installed on the Call Server.

## Loops (Common Equipment)

To configure or edit Loops (Common Equipment) information, select the **Loops** link in the **System** branch of the Element Manager navigator. The **Common Equipment** web page opens (see [Figure 39](#)).

**Figure 39**  
**Common Equipment web page**

Managing: [192.167.100.3](#)  
System > Loops (Common Equipment)

### Loops (Common Equipment)

**- Basic Configuration**

Input Description	Input Value
Change to Common Equipment parameters (CEQU) (TYPE)	<input type="text" value="CEQU"/>
Maximum Peripheral Equipment Density (MPED)	<input type="text" value="Octal (8D)"/>
Single Density Terminal equipment loop (TERM)	<input type="text"/> <input type="button" value="Edit"/>
Single Density Remote Peripheral Equipment loop (REMO)	<input type="text"/> <input type="button" value="Edit"/>
Double Density Terminal equipment loop (TERD)	<input type="text"/> <input type="button" value="Edit"/>
Double Density Remote Peripheral Equipment loop (REMD)	<input type="text"/> <input type="button" value="Edit"/>
Quadruple Density Terminal equipment loop (TERO)	<input type="text"/> <input type="button" value="Edit"/>
Quadruple density Remote Peripheral Equipment loop (REMO)	<input type="text"/> <input type="button" value="Edit"/>
Digital Trunk Channel Switches (DTCS)	<input type="text"/> <input type="button" value="Edit"/>
Extended Conference/TDS/MFS (XCT)	<input type="text" value="000 016"/> <input type="button" value="Edit"/>
Virtual Extended Conference/TDS/MFS (VXCT)	<input type="text" value="060 062"/> <input type="button" value="Edit"/>
Tone and Digit Switch (TDS)	<input type="text" value="*000 *016 *060 *062"/> <input type="button" value="Edit"/>
Multifrequency Sender loop (MFS)	<input type="text" value="*000 *016 *060 *062"/> <input type="button" value="Edit"/>
Conference loop (CONF)	<input type="text" value="*001 *017 *061 *063"/> <input type="button" value="Edit"/>
- Digital Trunk Interface Loop Number (DLOP)	<input type="button" value="Add New DLOP"/>

The **Common Equipment** web page contains buttons that act as links to additional web pages. The following functions can be performed from these pages:

- add and delete Tone and Digit Switch (TDS) numbers
- add and delete Digital Trunk Interface Loop (DLOP) numbers
- add and delete Conference loop (CONF) numbers
- configure parameters for the following Feature Packages:
  - Integrated Digital Access (Package 122)
  - 2 Mbit Digital Trunk Interface (Package 129)
  - Dial Tone Detection (Package 138)
  - 2.0 Mb/s Primary Rate Interface (Package 154)

The information entered in this section corresponds to CEQU (Common Equipment) data traditionally configured using LD 17 - Configuration Record 1.

To save changes made in this section, click **Submit** at the bottom of the **Common Equipment** web page.

## Superloops

To configure or edit Superloop information, select the **Superloop** link in the **System** branch of the Element Manager navigator. The **Superloop** web page opens as shown in [Figure 40 on page 113](#).

**Figure 40**  
**Superloops web page**

Managing: [207.179.153.99](#)  
System > Superloops

### Superloops

Choose a Superloop Number:  and type:

- Superloops: 0	Type: STD	<input type="button" value="Edit"/>
- Superloops: 4	Type: STD	<input type="button" value="Edit"/>
- Superloops: 8	Type: STD	<input type="button" value="Edit"/>
- Superloops: 12	Type: STD	<input type="button" value="Edit"/>
- Superloops: 16	Type: STD	<input type="button" value="Edit"/>
- Superloops: 32	Type: STD	<input type="button" value="Edit"/>
- Superloops: 36	Type: STD	<input type="button" value="Edit"/>
- Superloops: 40	Type: STD	<input type="button" value="Edit"/>
- Superloops: 44	Type: STD	<input type="button" value="Edit"/>
- Superloops: 48	Type: STD	<input type="button" value="Edit"/>
- Superloops: 64	Type: STD	<input type="button" value="Edit"/>
- Superloops: 68	Type: STD	<input type="button" value="Edit"/>
- Superloops: 72	Type: STD	<input type="button" value="Edit"/>
- Superloops: 96	Type: Virtual	<input type="button" value="Edit"/>
- Superloops: 100	Type: Phantom	<input type="button" value="Edit"/>
- Superloops: 128	Type: STD	<input type="button" value="Edit"/>
- Superloops: 132	Type: STD	<input type="button" value="Edit"/>

The information entered on this web page corresponds to the Superloop (SUPL) command available in LD 97 - Configuration Record 2.

To add a Superloop, choose a Superloop number and type (CARR, FIBR, IPMG, STD, Phantom, or Virtual) from the pull-down menu, then click to **Add**. The **Superloop Property Configuration** web page displays, as shown in [Figure 41 on page 114](#).

**Figure 41**  
**Superloop Property Configuration web page**

Managing: [192.167.100.3](#)  
System » [Superloops](#) » Superloops 0 Property Configuration

### Superloops 0 Property Configuration

Input Description	Input Value
Superloop (SUPL)	<input type="text" value="0"/>
Superloop Type (SUPT)	<input type="text" value="CARR"/>
Network Card is in Left or Right slot (SLOT)	<input type="text" value="LEFT"/> *
Extended Peripheral Equipment Controller (XPEC)	<input type="text"/> <span style="color: green;">Range: 1 - 95 *</span>

To save changes made in the Superloop properties, click **Submit** at the bottom of the web page.

To return to the **Superloop** web page, as shown in [Figure 40 on page 113](#), click the **Superloop** link in the navigation path at the top of the page.

To edit the properties of an existing Superloop, click the **Edit** button next to the Superloop entry on the **Superloops** web page. The **Superloop Property Configuration** web page for that Superloop opens.

To save changes made in the Superloop properties, click **Submit** at the bottom of the web page.

## SNMP

To configure or edit SNMP information, select the **SNMP** link in the **System** branch of the Element Manager navigator. The **SNMP Configuration** web page opens, as shown in [Figure 42](#).

**Figure 42**  
**SNMP Configuration web page**

Managing: 192.167.100.3  
System > SNMP Configuration

---

### SNMP Configuration

Input Description	Input Value
Navigation Site Name (NAV_SITE)	<input type="text"/>
Navigation System Name (NAV_SYSTEM)	<input type="text"/>
Contact Person for this machine (SNMP_SYSCONTACT)	<input type="text" value="System Contact"/>
Physical Location of this machine (SNMP_SYSLOC)	<input type="text" value="System Location"/>
Name assigned to this machine by the administrator (SNMP_SYSNAME)	<input type="text" value="System Name"/>
System Management Read community string (SYSMGMT_RD_COMM)	<input type="text" value="otm123"/>
System Management Write community string (SYSMGMT_WR_COMM)	<input type="text" value="otm123"/>
Admin Group community string (ADMIN_COMM)	1 <input type="text" value="public"/>
SNMP trap destination address (OPEN_ALARM)	0 <input type="text" value="IP address"/>

The information entered on this web page corresponds to the SNMP data traditionally configured using LD 117 - Ethernet and Alarm Management.

By entering information into the appropriate text boxes, the following tasks for SNMP can be performed:

- turn SNMP on and off by enabling or disabling traps
- trap destination IP addresses
- configure community name strings

- enable Call Server filtering
- enable Event Default Table (EDT), Event Preference Table (EPT), and alarm suppression thresholds

*Note:* Element Manager does not provide an SNMP alarm browser, so the OTM alarm browser must be used when SNMP alarm collection is required.

For detailed information on SNMP, see *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

## Geographic Redundancy

Geographic Redundancy is available only on CPP II and CPP IV systems.

To configure or edit Geographic Redundancy information, select the **Geographic Redundancy** option in the pull-down menu on the **Call Server Configuration** web page as shown in [Figure 43 on page 117](#). Then choose either the **Database Replication Control** or **State Control** option in the **Select Group** pull-down menu. Depending on the selection, either the **Database Replication Control** or **State Control** web page opens, as shown in [Figure 43 on page 117](#) and [Figure 44 on page 118](#).

**Figure 43**  
**Database Replication Control web page**

Managing **Buffv\_1 (47.11.139.4)**  
System > Geographic Redundancy > Database Replication Control

### Database Replication Control

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

On the **Database Replication Control** web page, users can configure:

- Backup Rule Number for Backup (BKUP\_RULE)
- Automatic Replication Backup (ABKUP)
- Backup rule number for Restore (RSTR\_RULE)
- Automatic Replication restore (ARSTR)
- Automatic Sysload (ASYSLD)

**Figure 44**  
**State Control web page**

Managing **Buffy 1 (47.11.139.4)**  
System > Geographic Redundancy > State Control

---

### State Control

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

On the **State Control** web page, users can configure:

- Geographic Redundancy Threshold (GRTHR)
- Short Term Failure Timeout in minutes (SFTO)
- Fault Clearance Timeout in minutes (FCTO)
- Secondary CS Deactivation Mode (SDAM)

The information entered on this web page corresponds to the commands available in LD 117.

For more information about Geographic Redundancy, see *Communication Server 1000: System Redundancy* (553-3001-307).

## Software

The **Software** link of the **System** branch of the Element Manager navigator can be used to perform patching of the Call Server or the Media Gateway.

### Call Server

Use Element Manager for Call Server patching as outlined in Procedure 2.

#### Procedure 2 Patching of Call Server

- 1 Click the **Software > Call Server** link in the **System** branch of the Element Manager navigator. The **PDT Password Portal** web page opens, as shown in [Figure 45](#).

**Figure 45**  
**PDT Password Portal web page**

Managing: **192.167.100.3**  
System » Software » PDT Password Portal

---

### PDT Password Portal

Please enter PDT password of Call Server then press button [Next]

Input Description	Input Value
PDT Password (PDT_PWD):	<input style="width: 100%;" type="text"/>

- 2 Enter the PDT Password and click **Next**.

The **Call Server** web page opens, as shown in [Figure 46 on page 120](#).

————— **End of Procedure** —————

**Figure 46**  
**Call Server web page**

**Call Server**

User PEPs       Dependency lists

PEP Setting		PEP Bin (Total: 0; Limit: 15)	
PEP File Name	<input type="text"/> <input type="button" value="Browse..."/>		
Days PEP vulnerable to sysload	<input type="text" value="3"/>	<input type="button" value="..&gt;&gt;"/>	
In service initialize threshold	<input type="text" value="5"/>	<input type="button" value="&lt;&lt;--"/>	
In service days to monitor inits	<input type="text" value="7"/>		<input type="button" value="Load and Activate"/>

Select Command	PEP ID	Apply to All	
PEP Status (PSTAT) <input type="button" value="v"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Submit"/>

```

Patch handle: 0*
  Filename: /u/patch/p20431_1.cpp
  Dependency List: None
  Dependency List Issue:
  Patch version: 0.60
  Reference number: ISS1:10F1
  Patch is in-service
  In-service date:          21/06/2005 09:16:21
  Last out-of-service date: never
  Patch is retained
  Patch retain level: RES
  
```

From the **Call Server** web page, the user can:

- load and activate a new PEP
- get the status of a single PEP or all PEPs (PSTAT)
- activate a single PEP or all PEPs (PINS)
- deactivate a single PEP or all PEPs (POOS)
- remove a single PEP or all PEPs (POUT)
- view the details on a PEP (PLIS)

The **PEP Setting** section at the top left of the web page enables the user to select files and choose settings. Clicking the right arrow (->>) button moves

PEP files into the **PEP Bin** section. Clicking the left arrow (<<-) button moves PEP files out of the **PEP Bin** section. Click the **Load and Activate** button to submit the selected PEP(s) to the call server. Results are displayed at the bottom of the screen.

*Note:* The user can download only 15 PEP files at a time. To install more than 15 PEPs on a single entity, the user must run the utility again.

All PEP commands require the PEP ID. After selecting the **PEP** command from the drop-down list, enter the **PEP ID** in the text box.

The **Apply to All** check box is enabled for all commands with the exception of the PLIS command. Clicking the **Submit** button executes the command. Results are displayed at the bottom of the screen.

Product Enhancement Package (PEP) Management can be applied to Call Servers. Element Manager enables users to load Matrix DepLists (MDP) to the Call Server and manage the MDPs using the Management DepList commands. Click the **Dependency lists** radio button. See [Figure 47 on page 122](#).

**Figure 47**  
**Call Server web page - Dependency Lists**

Managing: **Buffv\_1 (47.11.139.4)**  
 System > Software > PDT Password Portal > Call Server

---

**Call Server**

User PEPs     **Dependency lists**

**Dependency list Setting**

Dependency list File Name

Select Command	DepList Name	
DEPLIST Load (DLOAD) <input type="button" value="v"/> Days PEP vulnerable to sysload <input type="text" value="3"/> In service initialize threshold <input type="text" value="5"/> In service days to monitor inits <input type="text" value="7"/>	<input type="text" value="All"/> <input type="button" value="v"/>	<input type="button" value="Submit"/>

Call Server:  
 -----  
 System has no loaded Dependency Lists.

PEP lists are populated with individual PEPs contained in the update when a Matrix DepList is opened. The **Refresh** command refreshes the contents of an MDP on a target system and enables the user to load MDPs properly.

PEP Management supports the following commands:

- load and activate a new PEP
- get the status of a single PEP or all PEPs (DSTAT)
- activate a single PEP or all PEPs (DINS)
- deactivate a single PEP or all PEPs (DOOS)
- remove a single PEP or all PEPs (DOUT)
- view the details on a PEP (DLIS)

Each PEP in the Matrix DepList has its own PEP handle and can be uninstalled, like current multipatch functionality.

**WARNING**

Service updates that contain many PEPs can take time to install. The session time-out must be modified to ensure normal operation.

## Media Gateway

Patching of the Media Gateway or MG 1000S can be performed using Element Manager. Follow the steps in Procedure 3 to patch files on the MG 1000S.

### Procedure 3 Patching of the MG 1000S

- 1 Click the **Software > Media Gateway** link in the **System** branch of the Element Manager navigator.

If, during the current session, the PDT Password has not been entered, the **PDT Password Portal** web page opens.

Enter the PDT password, and click **Next**.

The **Media Gateway** web page opens, as shown in [Figure 48 on page 124](#).

- 2 Select one of the check boxes at the top of the web page to select the required Media Gateway for patching.

**Note:** If no Media Gateway is selected, the PEP command is applied to all the Media Gateways.

---

**End of Procedure**

---

**Figure 48**  
**Media Gateway web page**

Managing [Buffly 1 \(47.11.139.4\)](#)  
 System > Software > Media Gateway

### Media Gateway

Media Gateway	<input type="text"/>	Apply to All <input checked="" type="checkbox"/>	
PEP Setting		PEP Bin (Total: 0; Limit: 15)	
PEP File Name <input type="text"/>	<input type="button" value="Browse..."/>	<div style="border: 1px solid black; width: 100%; height: 100%;"></div> <input type="button" value="Load and Activate"/>	
Days PEP vulnerable to sysload	<input type="text" value="3"/>		<input type="button" value="-&gt;&gt;"/> <input type="button" value="&lt;&lt;-"/>
In service initialize threshold	<input type="text" value="5"/>		
In service days to monitor inits	<input type="text" value="7"/>		
Select Command		<input type="button" value="Submit"/>	
Automatic Centralized PEP Distribution(ACPD) Show <input type="button" value="Submit"/>			
Select Command	PEP File Name	Apply to All	<input type="button" value="Submit"/>
PEP In-Service (CPINS) <input type="button" value="Submit"/>	<input type="text"/>	<input type="checkbox"/>	

```

ACPD Status: Idle
+-----+
| Automatic Centralized PEP Distribution (ACPD) |
+-----+
| CAB | STATE | STATUS | LAST RUN TIME |
+-----+

```

From the **Media Gateway** page, the user can:

- load and activate a new PEP
- get the status of a single PEP or all PEPs (CPSTAT)
- activate a single PEP or all PEPs (CPINS)
- deactivate a single PEP or all PEPs (CPOOS)
- remove a single PEP or all PEPs (CPOUT)
- view the details on a PEP (CPLIS)

The **PEP Setting** section at the top left of the screen enables the user to select files and choose settings. Clicking the ->> (right arrow) button moves PEP files into the **PEP Bin** section. Clicking the <<- (left arrow) button moves PEP files out of the **PEP Bin** section. Click the **Load and Activate** button to

submit the selected PEP(s) to the Media Gateway. Results are displayed at the bottom of the screen.

*Note:* The user can download only 15 PEP files at a time. To install more than 15 PEPs on a single entity, the user must run the utility again.

All PEP commands require the PEP File Name. After selecting the **PEP** command from the drop-down list, enter the PEP File Name in the text box.

The **Apply to All** check box is enabled for all commands with the exception of the CPLIS command. Clicking the **Submit** button executes the command. Results are displayed at the bottom of the screen.



---

# IP Telephony

---

## Contents

This section contains information on the following topics:

Introduction . . . . .	128
IP Telephony . . . . .	128
Nodes: Servers, Media Cards . . . . .	128
General Commands . . . . .	129
Report Log . . . . .	132
System log . . . . .	134
Operational Measurement Reports . . . . .	136
Virtual Terminal . . . . .	137
Node Configuration . . . . .	139
Zones . . . . .	146
Network Address Translation (NAT) . . . . .	155
Quality of Service Thresholds (QoS) . . . . .	156
QoS Zone Basis Threshold Parameters relationship to QoS Call Basis Threshold Parameters . . . . .	157
TFS016 QoS IP statistics report information . . . . .	158
Personal Directories . . . . .	161
Software . . . . .	162
File Upload . . . . .	162
Telephony Firmware . . . . .	162
Servers and Media Cards . . . . .	162

## Introduction

The **IP Telephony** branch of the Element Manager navigator enables the user to view the version of software that is installed on the elements. The user can also upgrade IP Telephony loadware and distribute IP Telephony firmware to IP Telephony cards. The File Upload feature enables users to store loadware and firmware files on the Signaling Server.

## IP Telephony

### Nodes: Servers, Media Cards

Click the **Nodes: Servers, Media Cards > Maintenance and Reports** link in the **IP Telephony** branch of the Element Manager navigator to open the **Node Maintenance and Reports** web page, as shown in [Figure 49](#).

**Figure 49**  
Node Maintenance and Reports web page

Managing: **192.167.100.3**  
IP Telephony > Nodes: Servers, Media Cards > Node Maintenance and Reports

---

### Node Maintenance and Reports

- **Node ID: 7** Node IP: 192.167.101.3 Total elements: 3

Index	ELAN IP	Type	TN	ELAN					
<b>CS1000EN1</b>	192.167.100.4	Signaling Server	NO TN	GEN CMD	RPT LOG	OM RPT	Reset	Virtual Terminal	Status
<b>SigServFollower</b>	192.167.100.6	Signaling Server	NO TN	GEN CMD	RPT LOG	OM RPT	Reset	Virtual Terminal	Status
<b>VMG402</b>	192.167.100.7	Voice Gateway Media Card	4 0 2 0	GEN CMD	SYS LOG	OM RPT	Reset	Virtual Terminal	Status

Click buttons to invoke a command

This web page contains information on configured Signaling Servers and IP Telephony cards and is arranged by node. Click the **plus sign (+)** beside the Node ID number to view the elements assigned to the node.

For more information on IP Telephony, see *IP Line: Description, Installation, and Operation* (553-3001-365).

Seven buttons are located to the right of the TN column for each IP Telephony element:

- **GEN CMD** — Launches the **General Commands** web page.
- **RPT LOG** — Launches the **Report Utility** web page (for Signaling Servers).
- **SYS LOG** — Launches the **System log file** web page (for IP Telephony Cards).
- **OM RPT** — Launches the **Operational Management Report** web page.
- **Reset** — Resets the element.

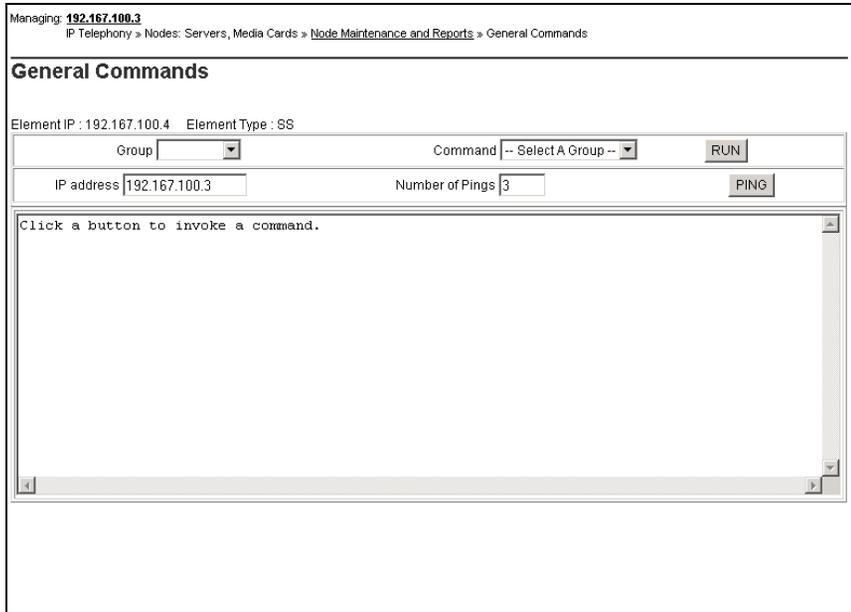
*Note:* When resetting the Signaling Server on which the web server is located, wait approximately five minutes before logging in again.

- **Virtual Terminal**— Opens a Telnet connection to the element over the Telephony Local Area Network (TLAN) subnet using the element's IP Address.
- **Status** — Displays the status of the element.

## General Commands

Click the **GEN CMD** button, located beside the information for an IP Telephony element as shown in [Figure 49 on page 128](#), to open the **General Commands** web page for that element. See [Figure 50 on page 130](#).

**Figure 50**  
**General Commands web page**



From this web page, users can issue commands to selected groups.

To issue an IP Line application command:

- 1 Select a group from the left-hand **Group** drop-down list. The corresponding commands for that group display in the **Command** drop-down list.
- 2 Select a **Command** from the **Command** drop-down list.
- 3 Click **Run**.  
The results appear in the box at the bottom of the web page.

Commands related to the node password are:

- nodePwdDisable - disables the node password
- nodePwdEnable - enables the node password

- `nodePwdShow` - displays the node password
- `nodeTempPwdClear` - clears the temporary node password
- `nodePwdSet` — sets the node password
- `nodeTempPwdSet` — sets the temporary node password

Passwords must conform to certain compositional rules.

To set the node password:

- 1 Select **nodePwdSet** from the drop-down list.
- 2 Enter the password in the **Node Password** text box.  
The password must be 6 - 14 characters in length. Valid entries are digits 0 through 9, and special character \*.
- 3 Select **nodePwdSet** from the drop-down list.
- 4 Click **Set**.

If a non-zero length password is configured, all IP Phones that attempt to register after the password is set display a prompt requesting the node password before enabling the TN to be modified.

A temporary node password can be configured to give temporary user access to the TN for configuration. A temporary node password removes the need to distribute the node password and the requirement to change it afterwards. The temporary node password automatically deletes itself after it has been used the defined number of times or when the duration expires, whichever comes first.

To set a temporary node password:

- 1 Select **nodeTempPwdSet** from the drop-down list.
- 2 Enter the temporary password in the **Node Password** text box.  
The password must be 6 - 14 characters in length. Valid entries are digits 0 through 9, and special character \*.

- 3 Enter the number of times that you want to enable the temporary password to be used in the **Uses** text box (maximum is 1000 times).
- 4 Enter the duration, in hours, for the temporary password in the **Time-out** text box (maximum is 240 hours).
- 5 Select **nodeTempPwdSet** from the drop-down list.
- 6 Click **Set**.

From the **General Commands** web page, any IP address can be pinged from this element. The default IP address is the address of the Call Server.

To ping an IP address:

- 1 Verify that the entry in the IP address text box is correct.
- 2 Enter the number of pings that to send in the **Number of Pings** text box.
- 3 Click **Ping**.

## Report Log

Click the **RPT LOG** button, located beside the information for the Signaling Server as shown in [Figure 49 on page 128](#), to open the **Node Report Logs** web page for the Signaling Server (see [Figure 51](#)).

**Figure 51**  
**Node Report Logs web page**

Managing: **192.167.100.3**  
 IP Telephony » Nodes: Servers, Media Cards » Node Maintenance and Reports » Node Report Logs

### Node Report Logs

Element IP : 192.167.100.4    Element Type : SS

<input type="button" value="RDOPEN"/>		<input type="button" value="RDSHOW"/>	
<input type="button" value="RDTAIL"/>		<input type="button" value="RDHEAD"/>	
Display Record Number	<input type="text" value="1000"/>	<input type="button" value="RDGO"/>	
Skip Records	<input type="text" value="0"/>	Display Records	<input type="text" value="1"/> <input type="button" value="RD"/>
Skip Records	<input type="text" value="0"/>	Display Records	<input type="text" value="1"/> <input type="button" value="RDS"/>
Start Record Number	<input type="text" value="0"/>	Display Records	<input type="text" value="1"/> <input type="button" value="VIEW"/>

Click a button to invoke a command.

The four buttons at the top of this web page provide one-click access to the following functions:

- **RDOPEN** — Opens the latest report file.
- **RDSHOW** — Shows a summary of the report file.
- **RDTAIL** — Shows  $x$  records up to the newest record in the report file (where  $x$  is the configured display size).
- **RDHEAD** — Shows  $x$  records starting from the oldest record in the report file (where  $x$  is the configured display size).

To view selected detail data on records in the report file, use the text boxes, the drop-down lists, and the following buttons:

- **RDGO** — Displays the record specified in the adjacent text box (where -1 is the oldest record and 1000 is the most recent).

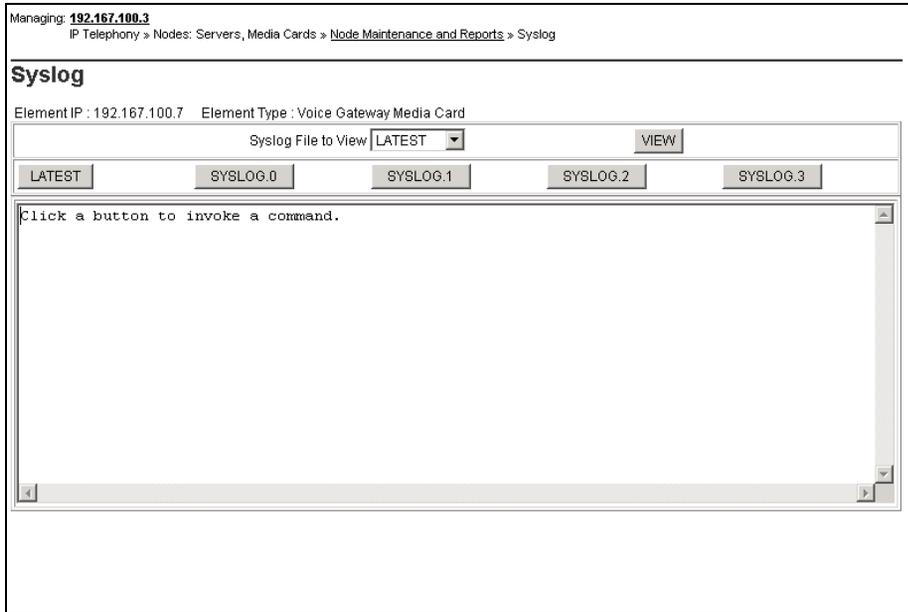
- **RD** — Browses the report records. Enter the number of records to skip and the number of records to display in the adjacent text boxes.
- **RDS** — Browses the report records with (symbolic) memory dump. Enter the number of records to skip, and select the number of records to display using the adjacent text box and drop-down list.
- **VIEW** — Views selected records. Enter a starting record number and select the number of records to view using the adjacent text box and drop-down list. Negative numbers indicate records previous to the starting record.

The results are displayed in the box at the bottom of the web page.

## System log

Click the **SYS LOG** button, located beside the information for an IP Telephony card, to open the **Syslog** web page for the IP Telephony card, as shown in [Figure 52 on page 135](#).

**Figure 52**  
**Syslog web page**



To view a System log file:

- 1 Select a file using the **Syslog File to View** drop-down list.
- 2 Click **VIEW**.

Alternatively, click one of the five buttons below the Syslog File to view the dialog box:

- **LATEST** — Displays the most recent record in the system log file.
- **SYSLOG.0** — Displays the file `/C:/log/syslog.0` located on the Media Card.
- **SYSLOG.1** — Displays the file `/C:/log/syslog.1` located on the Media Card.

- **SYSLOG.2** — Displays the file /C:/log/syslog.2 located on the Media Card.
- **SYSLOG.3** — Displays the file /C:/log/syslog.3 located on the Media Card.

The contents of the file appears in the box at the bottom of the web page.

## Operational Measurement Reports

The **OM** (Operational Measurement Report) **RPT** button enables users to view OM information. Click the **OM RPT** button, located beside information for an IP Telephony element as shown in [Figure 49 on page 128](#), to open the **OM Reports** web page for that element, as shown in [Figure 53](#).

**Figure 53**  
**OM Reports web page**

Managing: **192.167.100.3**  
 IP Telephony > Nodes: Servers, Media Cards > [Node Maintenance and Reports](#) > View OM FileType: Signaling Server, ELAN IP: 192.167.100.4

---

**View OM FileType: Signaling Server, ELAN IP: 192.167.100.4**

Select File	File Name	Create Time
<input checked="" type="radio"/>	u/om/omreport.153	SAT JUN 04 00:00:00 2005
<input type="radio"/>	u/om/omreport.154	SUN JUN 05 00:00:00 2005
<input type="radio"/>	u/om/omreport.155	MON JUN 06 00:00:00 2005
<input type="radio"/>	u/om/omreport.156	TUE JUN 07 00:00:00 2005
<input type="radio"/>	u/om/omreport.157	WED JUN 08 00:00:00 2005
<input type="radio"/>	u/om/omreport.158	THU JUN 09 00:00:00 2005
<input type="radio"/>	u/om/omreport.159	FRI JUN 10 00:00:00 2005
<input type="radio"/>	u/om/omreport.160	FRI JUN 10 14:00:00 2005

Click a button to invoke a command.

To view an OM Report file:

- 1 In the Select File column, click the option button beside the OM Report to be viewed.

*Note:* The limit of OM Report files is eight. Only the eight most recent OM Report files are available on the system.

- 2 Click **View OM File**.

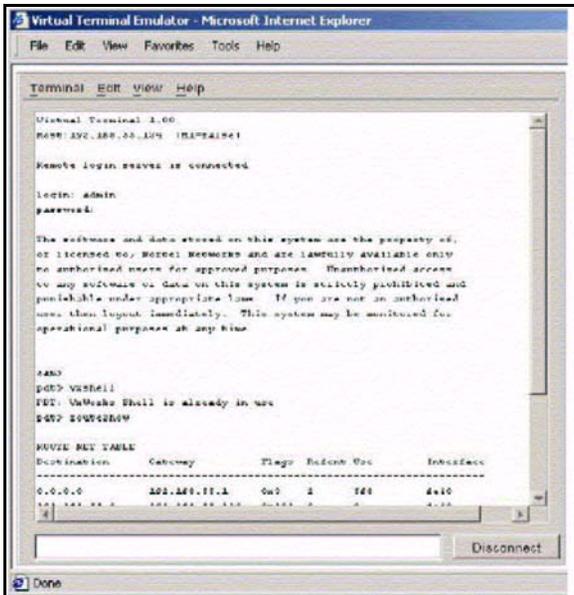
The contents of the file appear in the box at the bottom of the web page.

## Virtual Terminal

The Virtual Terminal is an integral part of the enhanced navigation tools for Element Manager.

Click the **Virtual Terminal** button on the **Node Maintenance and Reports** web page to open the **Virtual Terminal** window, as shown in [Figure 54 on page 138](#).

**Figure 54**  
**Virtual Terminal window**



The Virtual Terminal is a web-based window that enables access to the character-based interfaces supported by the components of the CS 1000 system, including all overlays not supported by Element Manager web pages. The Virtual Terminal can also be used to add new links to the system components or other Element Manager servers using the Bookmarks feature.

To access the Virtual Terminal for a particular IP device:

- 1 Choose the IP device you want to access on the **Node Maintenance and Reports** web page.
- 2 Click the **Virtual Terminal** button beside that node. The **Virtual Terminal** window opens, as shown in [Figure 54](#).
- 3 Enter the user name and password.

For more information about accessing and using the Virtual Terminal, refer to “Virtual Terminals” on [page 31](#).

## Node Configuration

To configure or edit Node Summary information, select the **Nodes: Servers, Media Cards > Configuration** link in the **IP Telephony** branch of the Element Manager navigator. The **Node Configuration** web page opens (see [Figure 55](#)).

**Figure 55**  
**Node Configuration web page**

Managing: **192.167.100.3**  
IP Telephony » Nodes: Servers, Media Cards » Node Configuration

---

### Node Configuration

New Node

- Node: 7 Node IP: 192.167.101.3	Edit	Transfer / Status	Delete
Voice LAN (TLAN) IP address	TN		
<b>Signaling Server</b>			
192.167.101.2			
192.167.101.4			
<b>Pentium Card</b>			
<b>Voice Gateway Media Card</b>			
192.167.101.5	4 0 2 0	<input type="button" value="VGW Channels"/>	

This web page also contains buttons that link to additional web pages. Follow these links to:

- add a new node
- import node files
- edit node configuration
- view the status of a previous transfer operation, or re-transfer to selected or failed elements

- delete a node
- add and edit Voice Gateway Channel (VGWC) configuration data on the media cards

To add a new node, enter a number in the **New Node** text box, and click **to Add**.

**IMPORTANT!**

Make sure that the values for the Node ID in Element Manager/IP Telephony and in the Call Server/Route Data Block (for the Virtual Trunk) are the same. If these Node ID values do not match, the IP Peer H.323 virtual trunks do not establish.

To edit the configuration information on an existing node, click **Edit** located to the right of the node's IP address.

To import a node file, follow the steps in Procedure 4:

**Procedure 4**  
**Importing node files**

- 1 Click **Import Node Files**.
- 2 Enter the ELAN (management LAN) network interface IP Address of the Leader in the text box. This address is used to retrieve the node files.
- 3 Click **Import**.  
If the import is successful, information appears in the text area of the Node Import Files screen and a message box appears.
- 4 In the message box, click **OK** to proceed to the **Node Summary** web page, where edit node information can be viewed.

---

**End of Procedure**

---

If any element within the Node fails to transfer either bootp or config files, the **TRANSFER/STATUS** button is highlighted in red. It is not necessary to manually retransfer the files; the next time the pbxlink is opened to that element, the files are updated. The **TRANSFER/STATUS** button is

highlighted in yellow if the transfer status of the node elements is unavailable. Clicking this button opens the **Transfer/Status** web page as shown in Figure 56.

**Figure 56**  
**Transfer/Status web page**

Managing: **192.167.100.3**  
IP Telephony > Nodes: Servers, Media Cards > [Node Configuration](#) > IP Telephony: Node ID 7 > Transfer / Status

### Transfer / Status

<input type="button" value="Select All"/> <input type="button" value="Unselect All"/> <input type="button" value="Transfer to Selected Elements"/>						
Hostname	ELAN IP	TN	Type	Role	Transfer Status (BOOTP)	Transfer Status (CONFIG)
<input type="checkbox"/> CS1000EN1	192.167.100.4		Signaling Server	Leader	Finished	Finished
<input type="checkbox"/> SigServFollower	192.167.100.6		Signaling Server	Follower	Finished	Finished
<input type="checkbox"/> VMG402	192.167.100.7	4 0 2 0	Voice Gateway Media Card	Follower	Finished	Finished

This web page displays the previous status of the node, and the failure reason for elements in nodes that failed to retrieve configuration files (*bootp.tab* and *config.ini*) from the Call Server side. Node elements that did not retrieve configuration files continue to display on the transfer progress status web page when the IP Telephony node configuration file is submitted and transferred.

The **Transfer/Status** web page displays two buttons:

- **Transfer to Selected Elements** — re-transfers node configuration files only to selected elements, regardless of a “Transfer Failed” state.
- **Transfer to Failed Elements** — transfers node configuration files to elements in a “Transfer Failed” state.

*Note:* The **Transfer to Failed Elements** button appears only when at least one element on the node failed to transfer either a *bootp.tab* or *config.ini* file in the previous operation. See [Figure 57](#).

**Figure 57**  
**Transfer/Status web page - Failed**

Managing: 207.179.153.99  
 IP Telephony » Nodes: Servers, Media Cards » Node Configuration » IP Telephony: Node ID 8 » Transfer / Status

**Transfer / Status**

Select All   Unselect All   Transfer to Selected Elements  
 Transfer to Failed Elements

Hostname	ELAN IP	TN	Type	Role	Transfer Status (BOOTP)	Transfer Status (CONFIG)
<input type="checkbox"/> NODE8	207.179.153.100		Signaling Server	Leader	Finished	Finished
<input type="checkbox"/> 1	207.179.153.109	13 0	ITG Pentium	Follower	Element Unreachable	Element Unreachable
<input type="checkbox"/> 2	207.179.153.111	12 0	Succession Media Card	Leader	Finished	Finished

Cancel

*Note:* To ensure the element has correct configurations, when an element is deleted, it should be reconfigured in a node with relevant necessary configurations, or physically removed from the network.

When clicking either the **to Add** button or any of the **Edit** buttons shown in the **Node Summary** web page, the **Edit** web page opens. See [Figure 58](#).

**Figure 58**  
**Edit web page**

Managing: 192.167.100.3  
IP Telephony > Nodes: Servers, Media Cards > Node Configuration > IP Telephony: Node ID 7 > Edit

### Edit

Save and Transfer Cancel

**- Node**

Node ID 7

Voice LAN (TLAN) Node IP address 192.167.101.3

Management LAN (ELAN) gateway IP address 192.167.100.1

Management LAN (ELAN) subnet mask 255.255.255.0

Voice LAN (TLAN) subnet mask 255.255.255.0

+ SNMP Add

+ VGW and IP phone codec profile

+ QoS

+ LAN configuration

+ SNTP

+ H323 GW Settings

+ Firmware

+ SIP GW Settings

+ SIP URI Map

+ SIP CD Services

+ Cards Add

From this web page, the following functions can be performed:

- view and edit basic Node information
- view and configure SNMP parameters and add IP addresses for forwarding SNMP traps
- view and configure VGW Profile data
- configure Quality of Service (QoS) data
- use LAN configuration to configure the ELAN Call Server IP Address, the Media Gateway IP Address, the ELAN and TLAN signaling ports and the ELAN and TLAN broadcast ports
- view and edit Simple Network Transfer Protocol (SNTP) Server and Client information

- view and configure file server access for downloading firmware for the IP Phones
- view and edit H.323 Settings
- view and edit SIP Gateway Settings, and configure the Re-direct Server
- perform SIP URI DN Mapping
- edit Converged Desktop Service information
- view and edit Signaling Server information
- view and edit card properties of Voice Gateway Media Cards

**IMPORTANT!**

Do not assign the same IP address for the Node ID and the TLAN network interface. The correct IP address must be verified manually. The Node IP address must be on the same subnet as the TLAN network interface IP addresses of the Voice Gateway Media Cards. Also, the Voice Gateway Media Card's TLAN and ELAN network interfaces must reside on separate logical subnets.

The IP Telephony Node Edit web page does not support multiple customers per node. SIP Converged Desktop Service and SIP URI to DN Mapping are configurable on a per-node basis. Only one customer is supported per node.

### **Enabling SIP**

Click the plus sign to the left of the **Signaling Servers** link on the **Edit** web page (see Figure 58 on [page 143](#)). Double-click the Signaling Server IP address. The **Signaling Server Properties** web page opens (see [Figure 59 on page 145](#)).

**Figure 59**  
**Signaling Server Properties web page**

- Signaling Server 192.167.100.4 Properties		Remove
Role	Leader	
Management LAN (ELAN) IP address	<input type="text" value="192.167.100.4"/>	
Management LAN (ELAN) MAC address	<input type="text" value="00:02:b3:ef:d5:cc"/>	
Voice LAN (TLAN) IP address	<input type="text" value="192.167.101.2"/>	
Voice LAN (TLAN) gateway IP address	<input type="text" value="192.167.101.1"/>	
Hostname	<input type="text" value="CS1000EN1"/>	
H323 ID	<input type="text" value="CS1000EN1"/>	
Enable set TPS	<input checked="" type="checkbox"/>	
Enable virtual trunk TPS	<input type="text" value="H.323 only"/>	
Enable SIP Proxy / Redirect Server	<input checked="" type="checkbox"/>	
SIP Transport Protocol	<input type="text" value="TCP"/>	
Local SIP Port	<input type="text" value="5060"/>	
SIP Domain name	<input type="text"/>	
SIP Gateway Endpoint Name	<input type="text"/>	
SIP Gateway Authentication Password	<input type="text"/>	
Enable H323 Gatekeeper	<input checked="" type="checkbox"/>	
Network Routing Service Role	<input type="text" value="Primary"/>	
System name	<input type="text" value="CS1000EN1"/>	

Choose a **mode** from the following options in the **Enable virtual trunk TPS** drop-down list:

- None
- H.323 only
- SIP only
- H.323 and SIP

Enter the SIP Transport Protocol, Local SIP Port, SIP Domain name, and SIP Gateway User user name and password.

When the administrator edits the Node and clicks **Save and Transfer**, transfer status information is updated and displayed.

Detailed procedures for performing these tasks are included in *IP Peer Networking: Installation and Configuration* (553-3001-213).

**Note:** The configuration of static Loss Plan values is performed using LD 73 instead of Element Manager. A Dynamic Loss Plan has been implemented to define the loss value per endpoint connection type. The loss plan adjusts the Voice Gateway Media Card gateway channel's loss for each call by sending pad values to the card.

### **Default values**

The default values in the system are for the North American loss plan.

### **Non-North American countries**

Installation of IP Line 4.5 in countries other than North American countries requires setting the pad values to that country's loss plan. If the system is installed in other countries, the Global PRI package (International 1.5/2.0 Mb/s Gateway package 167) must be used, and the NTP-specified values must be entered in LD 73. At the PDCA prompt, enter Table 15.

For more information on configuring Loss Plans, see *Transmission Parameters* (553-3001-182).

**Note:** When a system is installed in the UK, the CLI command UKLossPlanSet is entered at the CLI of one card in each node. This adjusts the loss plan of the IP Phones to the higher transmit levels required in the UK. For more information, see *IP Line: Description, Installation, and Operation* (553-3001-365).

## **Zones**

To configure or edit zone information, click the **Zones** link in the **IP Telephony** branch of the Element Manager navigator. The **Zones** web page opens (see [Figure 60 on page 147](#)).

**Figure 60**  
**Zones web page**

Managing: [192.167.100.3](#)  
IP Telephony > Zones

## Zones

**Maintenance**

- [Maintenance Commands for Zones \(LD 117\)](#)

**Configuration**

Please Choose the  to Add

---

- **Zone 0**
  - [Zone Basic Property and Bandwidth Management](#)
  - [Adaptive Network Bandwidth Management and CAC](#)
  - [Alternate Routing for Calls between IP Stations](#)
  - [Branch Office Dialing Plan and Access Codes](#)
  - [Branch Office Emergency Service Information](#)
  - [Branch Office Time Difference and Daylight Saving Time Property](#)

From this web page, add Zones by selecting a **Zone number** from the drop-down list and clicking **to Add**.

This web page also contains links to the four categories of Zone configuration data for each Zone configured. Click the plus sign to the left of next to the Zone number to see the following:

- Basic Property and Bandwidth Management
- Adaptive Network Bandwidth Management and CAC
- Alternate Routing for Calls between IP Stations
- Branch Office Dialing Plan and Access Codes
- Branch Office Emergency Service Information
- Branch Office Time Difference and Daylight Saving Time Property

For information on configuring the MG 1000B, see *Branch Office: Installation and Configuration* (553-3001-214).

To edit basic properties, click the **Zone Basic Property and Bandwidth Management** link. The **Zone Basic Property and Bandwidth Management** web page opens. See [Figure 61](#).

**Figure 61**  
**Zone Basic Property and Bandwidth Management web page**

Managing: **192.167.100.3**  
IP Telephony > [Zones](#) > Zone 0 > Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	0
Intrazone Bandwidth (INTRA_BW):	10000
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	10000
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

Submit Refresh Delete Cancel

The information entered on this web page corresponds to the ZONE, ZBRN, and ZDES data traditionally configured using LD 117 - Ethernet and Alarm Management.

To save changes made in **Zone Basic Property and Bandwidth Management** parameters, click **Submit** at the bottom of the web page.

To return to the **Zones** web page, click the **Zones** link in the navigation path at the top of the web page.

To configure the Adaptive Network Bandwidth Management feature, click the **Adaptive Network Bandwidth Management and CAC** link. The **Adaptive Network Bandwidth Management and CAC** web page opens, as shown in [Figure 62](#).

*Note:* Do not configure ANBWM for Zone 0 or Virtual Trunk zones.

**Figure 62**  
**Adaptive Network Bandwidth Management and CAC web page**

Managing: [207.179.153.99](#)  
IP Telephony > [Zones](#) > Zone 1 > Adaptive Network Bandwidth Management and CAC

### Adaptive Network Bandwidth Management and CAC

Input Description	Input Value
Zone Number (ZONE):	<input type="text" value="1"/>
Enable Call Admission Control Feature (STATE):	<input type="checkbox"/>
QoS Response Time Increase (ZQRT):	<input type="text" value="10"/> Range: 1 to 100 %
QoS Response Time Interval (ZQRTI):	<input type="text" value="5"/> Range: 1 to 120 min
Warning Alarm Threshold (ZOWAT):	<input type="text" value="85"/> Range: 1 to 99 %
Unacceptable Alarm Threshold (ZOUAT):	<input type="text" value="75"/> Range: 1 to 99 %
R Alarm Coefficient (CR):	<input type="text" value="50"/> Range: 1 to 100
Packet Loss Alarm Coefficient (CPL):	<input type="text" value="50"/> Range: 1 to 100
Delay Alarm Coefficient (CD):	<input type="text" value="50"/> Range: 1 to 100
Jitter Alarm Coefficient (CJ):	<input type="text" value="50"/> Range: 1 to 100
Coefficient for QoS (CQoS):	<input type="text" value="50"/> Range: 1 to 100
Record Validity Time Interval (CACVT):	<input type="text" value="48"/> Range: 1 to 255 hours

If the Adaptive Network Bandwidth Management feature is enabled using the **Enable Call Admission Control Feature (STATE)** check box, then the other parameters can be adjusted as required:

- QoS Response Time Increase (ZQRT) - Bandwidth limit increment, as a percentage of the QoS factor for the zone
- QoS Response Time Interval (ZQRTI) - Time (in minutes) between bandwidth limit increments

- Warning Alarm Threshold (ZQWAT) - A QoS value, which is lower than this value, but higher than the Critical (Unacceptable) Alarm Threshold, triggers a Major Alarm.
- Critical Alarm Threshold (ZQUAT) - A QoS value, which is lower than this value, triggers an Unacceptable (Critical) Alarm.
- R Alarm Coefficient (CR) - Value used to calculate the QoS value for the zone.
- Packet Loss Alarm Coefficient (CPL) - Value used to calculate the QoS value for the zone.
- Delay Alarm Coefficient (CD) - Value used to calculate the QoS value for the zone.
- Jitter Alarm Coefficient (CJ) - Value used to calculate the QoS value for the zone.
- Coefficient of QoS (CQoS) - Value used to calculate the overall QoS value for the zone.
- Recent Validity Time Interval (CACVT) - Amount of time (in hours) for zone-to-zone record validity. Once this interval expires, records for unused zones are purged from the tables.

To configure the Alternate Routing feature, click the **Alternate Routing for Calls between IP Stations** link. The **Alternate Routing for Calls between IP Stations** web page opens, as shown in Figure 63 on [page 151](#).

**Figure 63**  
**Alternate Routing for Calls between IP Stations**

Managing: [192.167.100.3](#)  
 IP Telephony » Zones » Zone 0 » Alternate Routing for Calls between IP Stations

---

### Alternate Routing for Calls between IP Stations

Input Description	Input Value
Zone Number (ZONE):	<input type="text" value="0"/>
Enable Alternate Routing Feature (ENL_ZALT):	<input type="checkbox"/>
Alternate Routing Prefix Digits (ALT_PREFIX):	<input type="text"/> Range: 0 to 9999999
Re-route for All Calls (ALL_CALLS):	<input type="checkbox"/>
Alarm Suppression Time Period (ZAST):	<input type="text"/> Range: 0 to 3600 Sec

Note: Alternate Routing (ALT) in combination with Adaptive Network Bandwidth Management (CAC) allows for maintaining QoS by rerouting interzone calls through alternate paths. Independently, Alternate Routing (ALT) is based on bandwidth exhaustion.

- Select the **Enable Alternate Routing feature (ENL\_ZALT)** check box to enable the Alternative Call Routing for NBWM feature.
- Enter a maximum of 7 digits in **Alternate Routing Prefix Digits (ALTPrefix)**.
- Select the **Re-route for All Calls (ALL\_CALLS)** check box to enable the feature for all calls.
- Click **Submit** to enter the data.

To edit dialing plan and access code parameters for a Zone's MG 1000B offices, click the **Branch Office Dialing Plan and Access Codes** link on the **Zones** web page. The **Zone Dialing Plan and Access Codes** web page opens. See [Figure 64 on page 152](#).

**Figure 64**  
**Zone Dialing Plan and Access Codes web page**

Managing: [192.167.100.3](#)  
IP Telephony » [Zones](#) » Zone 0 » Zone Dialing Plan and Access Codes

---

### Zone Dialing Plan and Access Codes

Input Description	Input Value
Zone Number (ZONE):	<input type="text" value="0"/>
Prefix (ACB_DC1):	<input type="text"/>
Country Code/Trunk Code (ACB_DC2):	<input type="text"/>
Destination Network Code (ACB_DC3):	<input type="text"/>
Dialed Access Code (ACB_LOC_AC):	<input type="text" value="No Access Code (NONE)"/>
New Access Code (ACB_LD_AC):	<input type="text" value="No Access Code (NONE)"/>

The information entered on this web page corresponds to the Zone Dialing Plan and Access Codes (ZACB) command available in LD 117 - Ethernet and Alarm Management.

To save changes made in **Zone Dialing Plan and Access Code** parameters, click **Submit** at the bottom of the web page.

To return to the **Zones** web page, click the **Zones** link in the navigation path at the top of the page.

To access emergency service parameters for a Zone's MG 1000B Offices, click the **Branch Office Emergency Service Information** link for the particular Zone on the **Zone List** web page. The **Zone Emergency Service Information** web page opens (see [Figure 65](#)).

**Figure 65**  
**Zone Emergency Service Information web page**

Managing: [192.167.100.3](#)  
IP Telephony » [Zones](#) » Zone 0 » Zone Emergency Service Information

---

### Zone Emergency Service Information

Input Description	Input Value
Zone Number (ZONE):	<input type="text" value="0"/>
Route number (ESA_ROUT):	<input type="text" value=""/>
ESA Access Code (ESA_AC):	<input type="text" value="None (AC0)"/>

The information entered on this web page corresponds to the Zone Emergency Service Information (ZESA) command available in LD 117 - Ethernet and Alarm Management.

To save changes made in **Zone Emergency Service** parameters, click **Submit** at the bottom of the web page.

To return to the **Zones** web page, click the **Zones** link in the navigation path at the top of the page.

To access the time difference and daylight saving time properties for a Zone's MG 1000B Offices, click the **Branch Office Time Difference and Daylight Saving Time Property** link on the **Zone List** web page. The **Time Difference and Daylight Saving Time Property** web page opens (see [Figure 66](#)).

**Figure 66**  
**Time Difference and Daylight Saving Time Property web page**

Managing: [192.167.100.3](#)  
 IP Telephony > Zones > Zone 0 > Time Difference and Daylight Saving Time

### Time Difference and Daylight Saving Time

**Time Difference Property**

Input Description	Input Value
Time Difference (TIME_DIFF):	<input type="text" value="0"/>

**Daylight Saving Time Property**

Input Description	Input Value
Zone Number (ZONE):	<input type="text" value="0"/>
Use Daylight Saving Time (USE_DST):	<input type="checkbox"/>
Active Status of Daylight Saving Time (DST_ACT):	<input type="text" value="No"/>
Start Month (START_MON):	January
Start Week (START_WEEK):	1
Start Day (START_DAY):	Monday
Start Hour (START_HOUR):	1
End Month (END_MON):	January
End Week (END_WEEK):	1
End Day (END_DAY):	Monday
End Hour (END_HOUR):	1

Submit Refresh Cancel

The information entered on this web page corresponds to the ZTDF and ZDST command data traditionally configured using LD 117 - Ethernet and Alarm Management.

To save changes made in Time Difference and Daylight Saving Time properties, click **Submit** at the bottom of the web page.

To return to the **Zones** web page, click the **Zones** link in the navigation path at the top of the page.

## Network Address Translation (NAT)

To configure or edit Network Address Translation (NAT) information, click the **Network Address Translation** link in the **IP Telephony** branch of the Element Manager navigator. The **Network Address Translation (NAT)** web page opens, as shown in [Figure 67](#).

**Figure 67**  
**Network Address Translation (NAT) web page**

Managing: **192.167.100.3**  
IP Telephony » Network Address Translation (NAT)

---

### Network Address Translation (NAT)

Input Description	Input Value	
Echo Server 1 IP Address	<input type="text" value="0.0.0.0"/>	
Echo Server 1 Port	<input type="text" value="10000"/>	Range: 1000 to 65535
Echo Server 2 IP Address	<input type="text" value="0.0.0.0"/>	
Echo Server 2 Port	<input type="text" value="10000"/>	Range: 1000 to 65535
NAT Session Timeout Value (seconds)	<input type="text" value="30"/>	Range: 20 to 600

Note: IP address 0.0.0.0 means that the default local Echo Server will be enabled

The information entered on this web page corresponds to data traditionally configured using LD 117 - Ethernet and Alarm Management.

To configure the Echo Server 1 and 2 IP addresses and port numbers, enter the values in corresponding input fields.

**Note:** Echo Server 1 and 2 default IP addresses use the TLAN network interface IP address of the LTPS card.

Enter the NAT session timeout value. Click the **Submit** button to save the changes. For more information, see *IP Line: Description, Installation, and Operation* (553-3001-365).

## Quality of Service Thresholds (QoS)

To configure or edit Quality of Service Threshold information, click the **Quality of Service Thresholds (QoS)** link in the **IP Telephony** branch of the Element Manager navigator. The **Quality of Service (QoS) Thresholds** web page opens (see [Figure 68](#)).

**Figure 68**  
Quality of Service (QoS) Thresholds web page

Managing: [192.167.100.3](#)  
IP Telephony » Quality Of Service (QoS) Thresholds

### Quality Of Service (QoS) Thresholds

QoS Zone Basis Threshold Parameters

Input Description	Input Value	Range
Zone Latency Warning Threshold (ZLWT):	<input type="text" value="20"/>	Range: 1 to 100 %
Zone Jitter Warning Threshold (ZJWT):	<input type="text" value="20"/>	Range: 1 to 100 %
Zone Packet Loss Warning Threshold (ZWPKL):	<input type="text" value="20"/>	Range: 1 to 100 %
Zone R Factor Warning Threshold (ZWR):	<input type="text" value="20"/>	Range: 1 to 100 %
Zone Latency Unacceptable Threshold (ZULAT):	<input type="text" value="2"/>	Range: 1 to 100 %
Zone Jitter Unacceptable Threshold (ZUJIT):	<input type="text" value="2"/>	Range: 1 to 100 %
Zone Packet Loss Unacceptable Threshold (ZUPKL):	<input type="text" value="2"/>	Range: 1 to 100 %
Zone R Factor Unacceptable Threshold (ZUR):	<input type="text" value="2"/>	Range: 1 to 100 %
Sample Rate Window (ZARW):	<input type="text" value="300"/>	Range: 60 to 3600 s
Minimum Sample Count (MSZW):	<input type="text" value="100"/>	Range: 50 to 1000

QoS Call Basis Threshold Parameters

Input Description	Input Value	Range
Call Latency Warning Threshold (WLAT):	<input type="text" value="40"/>	Range: 5 to 200 ms
Call Jitter Warning Threshold (WJIT):	<input type="text" value="20"/>	Range: 5 to 200 ms
Call Packet Loss Warning Threshold (WPKL):	<input type="text" value="20"/>	Range: 5 to 100 %

From this web page, Quality of Service (QoS) Thresholds can be viewed and edited. Every node in the system has the same threshold values.

The threshold parameters are grouped as follows:

- QoS Zone Basis Threshold Parameters
- QoS Call Basis Threshold Parameters

To save changes made to the threshold parameters, click **Submit** at the bottom of the web page.

**IMPORTANT!**

Changes to Quality of Service parameters do not take effect until a Call Server data dump is performed.

## QoS Zone Basis Threshold Parameters relationship to QoS Call Basis Threshold Parameters

The QoS Zone Basis Threshold Parameters allow for an overall level of alerts based on aggregated data for the zone. QoS samples are collected from active sets in the zone periodically by polling or received asynchronously, depending on the set firmware.

The statistics received are compared to the QoS Call Basis Threshold Parameters and violations are counted. The QoS Zone Basis Threshold Parameters define the level at which alarms are sent out. These indicate the percentage of the sets in the zone that exceed the defined per call thresholds for the different QoS metrics.

For example, if the zone unacceptable threshold for a particular metric is set to 2%, then zone alarms are issued for that metric if over 2% of the sets in the zone exceed the per call unacceptable threshold set for that metric.

Zone alarms are only issued if a minimum sample count is achieved during the zone-alarm-rate collection window (CHG SQOS command in LD 117).

The zone defaults for the warning items are higher than those for the unacceptable items (20% compared to 2%). The assumption is that the QoS Call Basis Thresholds are set at levels such that several warning alarms are normally issued.

An overall problem with the zone should only be indicated if there are a significant number of such violations. However, there should be almost no unacceptable alarms and it is appropriate that these be set to a far lower zone percentage threshold.

Nortel recommends you adjust the QoS Call Basis Threshold Parameters to a level appropriate for the installation. After that, set the QoS Zone Basis Threshold Parameters, taking into consideration the QoS Call Basis Threshold Parameters settings. If the QoS Call Basis Threshold Parameters are set low, then more violations are to be expected, and the QoS Zone Basis Threshold Parameters should be set higher to compensate. The converse is true for high per call threshold settings.

## TFS016 QoS IP statistics report information

The QoS IP statistics report, TFS016, reports on QoS and other IP statistics on a bandwidth zone basis for interzone and intrazone calls. This section explains how the QoS statistics are calculated.

### Basic calculation flow

- 1 The TPS in the Signaling Server polls IP Phones in an active call periodically to extract QoS statistics.
- 2 The statistics are collected for the duration of the call to build up a Quality Detail Record (QDR) which provides a summary of the call quality over the entire call.
- 3 If a call is modified (Transfer, Conference, Hold, Mute) a separate QDR is created for each segment of the call.
- 4 If one or both ends of the IP call are a VGMC (for example, DSP endpoint for IP to TDM conversion), the QDR records are built in the VGMC in a manner similar to the TPS.
- 5 At the end of the call, or call segment, the QDR record is sent to the Call Server to be accumulated into the traffic report.

The following metrics are calculated and reported. These metrics are with respect to the incoming media stream. The PVQM package is required for this functionality.

- **Latency**—Latency is calculated as per RFC 1889.

- **Jitter**—Jitter is calculated as per RFC 1889
- **Packet Loss**—Packet Loss is calculated as per RFC 1889.
- **R-Value**—The R-Value is the User R-Value and is calculated by the Telchemy VQMonEP software.  
Listening R factor is a direct measure of the call quality or transmission quality, and incorporates the effects of CODEC type, packet loss, discard, burstiness, or delay. Note that R-Value is only available from devices equipped with Telchemy software, such as Phase 2 sets.

For more information on metrics available for different endpoint types, see *Converging the Data Network with VoIP (553-3001-160)*.

The QDR records are built up during a call by polling the end point periodically to obtain a snapshot value for each metric. The QDR record has 3 counters for each metric labeled Good, Warning, and Unacceptable. This makes a total of 12 counters. At each polling interval each metric is examined and categorized into one of the categories—Good, Warning, Unacceptable—and the appropriate counter is incremented. At the completion of a call, all of the metrics have the same total number of counts (although the distribution may be different) and the total count is equal to the total number of polling intervals.

You set the thresholds for Good, Warning, and Unacceptable QoS levels. These are the same thresholds used for the per-call QoS alarms (set using LD 117 commands CHG CQWTH, CHG CQUTH).

At the end of a call, the QDR record is forwarded to the Traffic system which aggregates all of the QDR records on a per zone basis. The Traffic system maintains a similar set of 12 counters for each active bandwidth zone in the system. The counters for each incoming QDR record are added to the corresponding counters for the zone.

For each call, the QDR record is built up as follows:

- The QDR counts are cleared when the speech path is first established.
- Each IP Phone in an active call is polled periodically according to the polling interval configured (CHG SQOS, SamplePeriod, default 30sec).

- For each poll done, the metric for Latency, Jitter, Packet Loss, and R Value are classified into Good, Warning and Unacceptable, and the appropriate QDR record count is incremented. The QDR sample count is incremented by one.
- At the end of a call, another statistic is gathered as if a poll was done and the QDR record is updated. The QDR sample count is incremented by one.
- Phase 0/1 and i2050v1 sets do not generate asynchronous alarms, and alarms are determined by this same polling mechanism. Phase 2 sets and other sets issue asynchronous alarms (not determined by polling). A check is made of the QDR record for sets issuing asynchronous alarms to make the statistics correspond to the asynchronous alarms issued. Counts are kept of the QoS threshold violation alarms associated with the call. If a particular alarm statistic is greater than the corresponding count in the QDR (such as warning Latency count), then the QDR count is increased. The sample count is not incremented in this case.

After call completion, the QDR record is forwarded to the Call Server to be aggregated into the zone statistics. First, the Call Server determines if the QDR record is for interzone or intrazone to increment the appropriate statistics. The sample count in the QDR record is added to the zone sample count and the warning and unacceptable counts are accumulated similarly for the other metrics.

*Note:* The zone statistics are only updated with the QDR record at the end of a call, so there may be QoS alarms issued in one traffic period and the zone statistic reported in another period for a call that spans traffic periods.

The following tables show examples QoS warning settings.

QoS Zone Rate Threshold	Value
unacceptable Jitter	2
unacceptable Latency	2
unacceptable PacketLoss	2
unacceptable R Factor	2

QoS Zone Rate Threshold	Value
warning Jitter	20
warning Latency	20
warning PacketLoss	20
warning R Factor	20
Sample Window	300
Min Sample Count	100

QoS Call Basis Threshold	Value
unacceptable Jitter	40
unacceptable Latency	100
unacceptable PacketLoss	70
unacceptable R Factor	60
warning Jitter	20
warning Latency	40
warning PacketLoss	20
warning R Factor	65
Sample Period	30

## Personal Directories

The Personal Directories, Redial List, and Callers List feature runs on either a leader or follower Signaling Server. It can run on the same Signaling Server as Element Manager if the number of users is less than 1000. If the Signaling Server supports more than 1000 users, use a separate Signaling Server.

For more information on Personal Directories, Redial List, and Callers List, see *IP Line: Description, Installation, and Operation* (553-3001-365).

## Software

The **Software** link of the **IP Telephony** branch of the Element Manager navigator can be used to upload and store files, upgrade firmware, and perform patching activities.

### File Upload

The file upload function enables users to upload and store loadware and firmware files on the Signaling Server. These files can then be downloaded to IP Phones and other network elements, using the functions available under the **Software > Voice Gateway Media Card** and **Software > Telephony Firmware** links in the **IP Telephony** branch of the navigator.

For more information on the file upload function, see *IP Line: Description, Installation, and Operation* (553-3001-365).

### Telephony Firmware

The **Software > Telephony Firmware** link in the **IP Telephony** branch of the Element Manager navigator allows users to upgrade IP Phone firmware. For more information, see *IP Line: Description, Installation, and Operation* (553-3001-365).

### Servers and Media Cards

Click the **Software > Servers and Media Cards** link in the **IP Telephony** branch of the Element Manager navigator to open the **Servers and Media Cards** web page as shown in [Figure 69](#).

**Figure 69**  
**Servers and Media Cards web page**

Managing: **Butfy\_1 (47.11.139.4)**  
 IP Telephony > Software > Servers and Media Cards

### Servers and Media Cards

Signaling Server   
  ITG Pentium   
  Voice Gateway Media Card

PEP Setting		PEP Bin (Total: 0; Limit: 15)	
PEP File Name	<input type="text"/> Browse...	<div style="border: 1px solid black; width: 100%; height: 100%;"></div>	
Days PEP vulnerable to sysload	<input type="text" value="3"/>		
In service initialize threshold	<input type="text" value="5"/>		
In service days to monitor inits	<input type="text" value="7"/>	<input type="button" value="Load and Activate"/>	

Select Elements		
<input type="button" value="Open all nodes"/>	<input type="button" value="Close All nodes"/>	<input type="button" value="Clear all"/>

<b>- Node ID: 3437</b>		Node IP: 47.11.145.72		Total elements: 2
Index	ELAN IP	TN	Type	Role
<input checked="" type="checkbox"/>	gr2_sip_ss	47.11.139.8	NO TN	Signaling Server
				Leader
<input checked="" type="checkbox"/>	gr2_ss_follower	47.11.139.6	NO TN	Signaling Server
				Follower
				<input type="button" value="PSTAT"/>
<b>- Node ID: 3434</b>		Node IP: 47.11.145.76		Total elements: 3
Index	ELAN IP	TN	Type	Role
<input type="checkbox"/>	1	47.11.139.17	4 0 1 0	Voice Gateway Media Card
				Leader
<input type="checkbox"/>	2	47.11.139.13	0 0 9 0	Voice Gateway Media Card
				Follower
<input type="checkbox"/>	4	47.11.139.15	0 1 9 0	Voice Gateway Media Card
				Follower
				<input type="button" value="PSTAT"/>

From this web page the following functions can be performed:

- load and activate a new PEP
- view the status of a single PEP or all PEPs (PSTAT)
- activate a single PEP or all PEPs (PINS)
- deactivate a single PEP or all PEPs (POOS)
- remove a single PEP or all PEPs (POUT)
- view the details on a PEP (PLIS)

The **PEP Setting** section at the top left of the web page enables users to select files and choose settings.

## Procedure 5

### Loading and Activating PEP Settings to the Call Server

- 1 Click **Browse**.

The **Choose file** window opens.

- 2 Choose a file to be downloaded and click **Open**.
- 3 Enter the number of **Days PEP vulnerable to sysload**.
- 4 Enter the **In service initialize threshold**.
- 5 Enter the **In service days to monitor inits**.
- 6 Click the -->> (right arrow) button to move the PEP files into the **PEP Bin** section.
- 7 Click **Load and Activate** to submit the selected PEPs to the call server.

Results are displayed at the bottom of the screen.

---

#### End of Procedure

---

Clicking the <<-- (left arrow) button moves PEP files out of the **PEP Bin** section.

*Note:* A maximum of 15 PEP files can be downloaded at a time. If more than 15 PEPs must be installed on a single entity, the utility must be run again.

Click the **PSTAT** button to open the **Type** web page for the selected element. See [Figure 70 on page 165](#).

**Figure 70**  
**Type web page**

Managing: 192.167.100.3  
Type: Signaling Server, ELAN IP: 192.167.100.4

**Type: Signaling Server, ELAN IP: 192.167.100.4**

PEP Setting		PEP Bin (Total: 0; Limit: 15)	
PEP File Name	<input type="text"/> Browse...	<input type="text"/>	
Days PEP vulnerable to sysload	<input type="text" value="3"/>		
In service initialize threshold	<input type="text" value="5"/>		
In service days to monitor inits	<input type="text" value="7"/>		
		-->>	<<--
		Load and Activate	

Select Command	PEP ID	Apply to All	
PEP Status (PSTAT) ▾	<input type="text"/>	<input type="checkbox"/>	Submit

System has no loaded patches.

All PEP commands require the PEP ID. After selecting the PEP **Command** from the drop-down list, enter the **PEP ID** in the text box.

The **Apply to All** check box is enabled for all commands with the exception of the PLIS command. Clicking the **Submit** button executes the command. Results are displayed at the bottom of the screen.



---

# Customers, Routes and Trunks

---

## Contents

This section contains information on the following topics:

<a href="#">Introduction</a> .....	167
<a href="#">Customers</a> .....	167
<a href="#">Route and Trunk Configuration</a> .....	177
<a href="#">Routes and Trunks</a> .....	177
<a href="#">D-channels</a> .....	188
<a href="#">Digital Trunk Interface</a> .....	192

## Introduction

The **Customers** and **Routes and Trunks** branches of the Element Manager navigator are used to launch web pages that enable the user to configure and edit data relating to customers and their equipment.

## Customers

When the user clicks the **Customers** branch of the Element Manager navigator, the **Customers** web page opens, as shown in [Figure 71 on page](#)

168. To configure customer data, click the **Edit** button next to the customer to be configured.

**Figure 71**  
**Customers web page**

Managing: 192.167.100.3  
Customers

**Customers**

Choose a Customer Number: 3 to Add

- Customer: 0	Total routes: 1	Total trunks: 2	Edit
- Customer: 1	Total routes: 0	Total trunks: 0	Edit
- Customer: 2	Total routes: 0	Total trunks: 0	Edit

To add a new customer, select a number from the **Choose a Customer Number** drop-down list and click **to Add**.

The **New Customer Property Configuration** web page opens, as shown in [Figure 72 on page 169](#).

**Figure 72**  
**New Customer Property Configuration web page**

Managing: **192.167.100.3**  
 Customers > New Customer 3 Property Configuration

### New Customer 3 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Customer Data Block (CDB) (TYPE)	<input type="text" value="CDB"/>
Customer number (CUST)	<input type="text" value="3"/>
ANI Attendant Billing number (ANAT)	<input type="text"/> *
ANI Listed Directory Number (ANLD)	<input type="text"/> *
Options (OPT)	<input type="button" value="Edit"/>

- + Flexible Feature Codes (FFC\_DATA)
- + Feature options (FTR\_DATA)
- + Listed Directory Number options (LDN\_DATA)
- + ISDN and ESN Networking options (NET\_DATA)
- + Night service options (NIT\_DATA)
- + Feature Packages

\* *Mandatory fields of current configuration*

The Element Manager Customer Explorer offers a logical grouping of parameters. For example, when configuring a route data block, all parameters requiring mandatory inputs are grouped under the heading Basic Configuration. As an administrator starts making selections in the mandatory fields, additional parameters appear in the browser. Additional route data block parameters are grouped under the headings Flexible Feature Codes, Feature options, Listed Directory Number Options, ISDN and ESN Networking options, Night Service options, and Feature Packages.

The configuration of route and trunk data blocks is context-sensitive. Logical conditions are applied to each parameter associated with these data blocks to determine if the parameter should display in the web browser for a particular configuration. The conditions are executed every time an administrator makes a selection on a parameter. The number of parameters displayed is reduced so that those most relevant to the condition are displayed.

To edit customer, route, or trunk data, or to add new routes or trunks, click the appropriate link.

### Customer properties

Click the **Edit** button beside a Customer row, as shown in [Figure 71 on page 168](#), to open the **Customer Property Configuration** web page for that customer, as shown in [Figure 73](#).

The information entered in the **Basic Configuration** section of this web page corresponds to Default Customer Data Block information traditionally configured using LD 15 - Customer Data Block.

**Figure 73**  
Customer Property Configuration web page

Managing: [192.167.100.3](#)  
[Customers](#) » Customer 0 Property Configuration

### Customer 0 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Customer Data Block (CDB) (TYPE)	<input type="text" value="CDB"/>
Customer number (CUST)	<input type="text" value="0"/>
ANI Attendant Billing number (ANAT)	<input type="text" value="1000"/> *
ANI Listed Directory Number (ANLD)	<input type="text" value="221"/> *
Options (OPT)	<input type="button" value="Edit"/>

- + Flexible Feature Codes (FFC\_DATA)
- + Feature options (FTR\_DATA)
- + Listed Directory Number options (LDN\_DATA)
- + ISDN and ESN Networking options (NET\_DATA)
- + Night service options (NIT\_DATA)
- + Feature Packages

\* Mandatory fields of current configuration

In the **Basic Configuration** section of the web pages shown in [Figure 72 on page 169](#) and [Figure 73 on page 170](#), the following functions can be performed:

- Configure the Automatic Number Identification (ANI) billing number for attendants making ANI calls (ANAT).
- Configure the ANI Listed Directory Number (ANLD).
- Click the **Edit** button beside Options (OPT) to edit available options.

To save changes made in these sections, click **Submit** at the bottom of the web page.

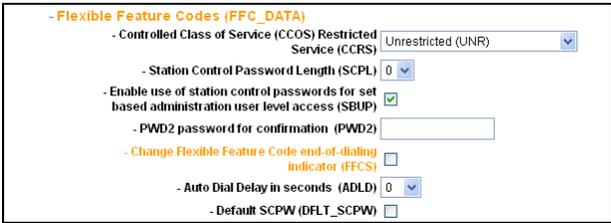
### Flexible Feature Codes configuration

Click the plus sign located to the left of the **Flexible Feature Codes (FFC\_DATA)** heading, to expand the section to show the parameters associated with Flexible Feature Codes (see [Figure 74](#)).

The information entered in the **Flexible Feature Codes** section of the **Customer Property Configuration** web page corresponds to FFC (Flexible Feature Code and options) data, traditionally configured using LD 15 - Customer Data Block.

This section of the web page also includes a sub-section that enables users to configure Change Flexible Feature Code end-of-dialing indicator (FFCS).

**Figure 74**  
**Flexible Feature Codes (FFC\_DATA) configuration**



- Flexible Feature Codes (FFC\_DATA)

- Controlled Class of Service (CCOS) Restricted Service (CCRS)
- Station Control Password Length (SCPL)
- Enable use of station control passwords for set based administration user level access (SBUP)
- PWD2 password for confirmation (PWD2)
- Change Flexible Feature Code end-of-dialing indicator (FFCS)
- Auto Dial Delay in seconds (ADLD)
- Default SCPW (DELT\_SCPW)

To save changes made in this section, click **Submit** at the bottom of the web page.

### Feature options configuration

Click the plus sign located to the left of the **Feature Options (FTR\_DATA)** heading to expand the section to show the parameters associated with Feature options, as shown in [Figure 75 on page 172](#).

The information entered in the **Feature Options** section of the **Customer Property Configuration** web page corresponds to FTR (Features and options) data traditionally configured using LD 15 - Customer Data Block.

This section of the web page also includes sub-sections that enable users to configure:

- Boss Secretary Filtering Enhancement (BSFE)
- Virtual Office Automatic Logout (VO\_ALO)
- Conference Display (CONF\_DSP)

**Figure 75**  
**Feature options (FTR\_DATA) configuration**

- Feature options (FTR\_DATA)

- Special Prefix number (SPRE)
- Network Authorization Code (NAUT)
- Internal/external definition (IDEF)
- Analog Semi-Permanent Connection re-connection Timer (ASPCT)  Range: 10 - 180
- Network Station Camp-On to sets on this node (MSCP)
- List Entry Number Delimiter (LEND)
- Mandatory Speed Call Delimiter (MSCD)
- Serial Data Interface Port Monitor (PORT)
- Personal Call Assistant (PCA)
- Target Personal Call Assistant DN (TPDN)

+ - Boss Secretary Filtering Enhancement (BSFE)

- Enable Virtual Office Automatic Logout (VO\_ALO)

+ - Change Conference Display configurations (CONF\_DSP)

To save changes made in this section, click **Submit** at the bottom of the web page.

## Listed Directory Number options configuration

Click the plus sign located to the left of the **Listed Directory Number options (LDN\_DATA)** heading, as shown in [Figure 73 on page 170](#), to expand the section to show the parameters associated with LDN options (see [Figure 76](#)).

**Figure 76**  
Listed Directory Number options (LDN\_DATA) configuration

- Listed Directory Number options (LDN\_DATA)  
 - Departmental listed directory number (yes/no) (LDN)   
 - Listed Directory Number 0 (LDN0)   
 - Listed DN 1 (LDN1)   
 - Listed DN 2 (LDN2)   
 - Listed DN 3 (LDN3)   
 - Listed DN 4 (LDN4)   
 - Listed DN 5 (LDN5)   
 - Attendant Incoming Indicators (ICI)

The information entered in the **Listed Directory Number options** section of the **Customer Property Configuration** web page corresponds to LDN (Listed Directory Number) data traditionally configured using LD 15 - Customer Data Block.

To save changes made in this section, click **Submit** at the bottom of the **Customer Property Configuration** web page.

## ISDN and ESN Networking options configuration

Click the plus sign located to the left of the **ISDN and ESN Networking options (NET\_DATA)** heading, as shown in [Figure 73 on page 170](#), to expand the section to show the parameters associated with networking options (see [Figure 77 on page 174](#)), including the Calling Line Identification (CLID) parameters.

The information entered in the **ISDN and Networking options** section of the **Customer Property Configuration** web page corresponds to NET (Networking) data traditionally configured using LD 15 - Customer Data Block.

**Figure 77**  
**ISDN and ESN Networking options (NET\_DATA) configuration**

- ISDN and ESN Networking options (NET\_DATA)

- Transfer on ringing of supervised external trunks (TRRX)
- CLID information for incoming/outgoing calls (OCLI)
- Connection of supervised external trunks (EXTT)
- Flexible Trunk to Trunk Connection Option (FTOP)
- Home DN (HMDN)
- Flexible Orbiting Prevention Timer (FOPT)
- Country Code (CNTC)
- National Access Code (NATC)
- International Access Code (INTC)

-- Calling Line Identification option (CLID)

- CLID entry size (SIZE)  Range: 0 - 4000
- Country code (INTL)
- CLID entry data (ENTRY\_GRP)

Click the **Add New** button in the **CLID** section to open the **CLID entry data Configuration** web page, as shown in [Figure 78](#).

**Figure 78**  
**CLID entry data Configuration web page**

Managing: 192.167.100.3  
 Customers > Customer 0 Property Configuration > Customer 0, -- CLID entry data Configuration

**Customer 0, -- CLID entry data Configuration**

**-- CLID entry data**

Input Description	Input Value
-- CLID entry to be configured (ENTRY)	<input type="text"/> *
-- National code for home national number (HNTN)	<input type="text"/>
-- Home Local Number for Emergency Services Access calls (ESA_HLCL)	<input type="text"/>
-- Home National Number for Emergency Services Access calls (ESA_INHN)	<input type="checkbox"/>
-- Append the originating Directory Number for Emergency Services Access calls (ESA_APDN)	<input checked="" type="checkbox"/>
-- Local code for home local number or Listed DN (HLCL)	<input type="text"/>
-- Use DN as DID (DIDN)	<input type="text" value="YES (YES)"/> <input type="button" value="v"/>
-- Home location code (HLOC_CLID)	<input type="text"/>
-- Local steering code (LSC_CLID)	<input type="text"/>
-- Send information to a CLASS set as the calling number (CLASS_FMT)	<input type="text" value="Send internal Directory Number (DN)"/> <input type="button" value="v"/>

Clicking on the **Return - - CLID entry data** button saves the changes and opens the **CLID entry** web page.

### Night service options configuration

Click the plus sign located to the left of the **Night service options (NIT\_DATA)** heading, as shown in [Figure 73 on page 170](#), to expand the section to show the parameters associated with the night service feature, as shown in [Figure 79](#).

**Figure 79**  
**Night service options (NIT\_DATA) configuration**

- Night service options (NIT\_DATA)

- Network Alternate Route Selection Interdigit Timer (NIT)
- First Night Service DN by Time of Day (NIT1)
- Hour and Minute for First Night Service DN (TIM1)
- Second Night Service DN by Time of Day (NIT2)
- Hour and Minute for Second Night Service DN (TIM2)
- Third Night Service DN by Time of Day (NIT3)
- Hour and Minute for Third Night Service DN (TIM3)
- Fourth Night Service DN by Time of Day (NIT4)
- Hour and Minute for Fourth Night Service DN (TIM4)

The information entered in the **Night Service options** section of the **Customer Property Configuration** web page corresponds to NIT (Night Service) data traditionally configured using LD 15 - Customer Data Block.

To save changes made in this section, click **Submit** at the bottom of the **Customer Property Configuration** web page.

### Feature Packages

Click the plus sign located to the left of the **Feature Packages** heading, as shown in [Figure 73 on page 170](#), to expand the section to show software feature packages (see [Figure 80 on page 176](#)).

**Note:** The only feature packages whose parameters can be viewed and edited are those that have been enabled on the CS 1000S or CS 1000M system. Feature packages cannot be removed or added from Element Manager.

Click the plus sign located to the left of the feature package name to view and edit the parameters associated with the feature package. For feature packages that are not equipped for the customer, Element Manager includes a button labeled **To Order**. This button provides a link to information on how to order the feature package.

**Figure 80**  
**Feature Packages**

- Feature Packages	
+ Do Not Disturb Individual	Package: 9
+ End-to-End Signaling	Package: 10
+ Message Waiting Center	Package: 46
+ New Flexible Code Restriction	Package: 49
+ Set Relocation	Package: 53
+ Network Alternate Route Selection	Package: 58
+ Distinctive Ringing	Package: 74
+ Departmental Listed Directory Number	Package: 76
+ Command Status Link	Package: 77
- Automated Modem Pooling	Package: 78 -- Unequipped <input type="button" value="To Order"/>
+ Pretranslation	Package: 92
+ Dialed Number Identification System	Package: 98
+ Malicious Call Trace	Package: 107
+ Incoming Digit Conversion	Package: 113
+ Directed Call Pickup	Package: 115
+ Enhanced Music	Package: 119
+ Station Camp-On	Package: 121
+ Integrated Digital Access	Package: 122
+ Digital Private Network Signaling System 1	Package: 123
+ Flexible Tones and Cadences	Package: 125
+ Multifrequency Compelled Signaling	Package: 128
+ International Supplementary Features	Package: 131
+ Enhanced Night Service	Package: 133

To save changes made in this section, click **Submit** at the bottom of the **Customer Property Configuration** web page.

**IMPORTANT!**

If configuring M3900 System Initiated Language (Package 386) and Japanese is selected as the default language, the user must explicitly configure the set-to-set-messages (MSG 1 to MSG10). Otherwise, the customer information does not load when clicking **Submit** and does not display.

## Route and Trunk Configuration

There are three options in the **Routes and Trunks** branch of the Element Manager navigator.

### Routes and Trunks

Click the **Routes and Trunks** link on the **Routes and Trunks** branch of the Element Manager navigator to open the **Routes and Trunks** web page, as shown in [Figure 81 on page 178](#). From this web page, users can view information on existing customers, routes, and trunks.

**Figure 81**  
**Routes and Trunks web page**

	Total routes:	Total trunks:	
+ Customer: 0	1	2	<input type="button" value="Add route"/>
- Customer: 1	0	0	<input type="button" value="Add route"/>
- Customer: 2	0	0	<input type="button" value="Add route"/>

This web page also contains buttons that link to additional web pages. Follow these links to

- add a new route
- edit route data
- add a new trunk
- edit trunk data
- delete multiple trunks

### **Route Properties**

Click the **Edit** button beside a Route row to open the **Route Property Configuration** web page for the selected customer and route. See [Figure 82 on page 179](#).

**Note:** If there are a large number of routes or trunks, this web page can be slow to load.

The information entered in the **Basic Configuration** section of this web page corresponds to Route Data Block information traditionally configured using LD 16 - Route Data Block.

**Note:** H.323 and SIP must not use the same route.

For information on configuring routes, see *IP Peer Networking: Installation and Configuration (553-3001-213)*.

**Figure 82**  
**Route Property Configuration web page**

Managing: **192.167.100.3**  
Routes and Trunks > [Routes and Trunks](#) > Customer 0, Route 1 Property Configuration

---

### Customer 0, Route 1 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Route Data Block (RDB) (TYPE)	<input type="text" value="RDB"/>
Customer number (CUST)	<input type="text" value="00"/>
Route Number (ROUT)	<input type="text" value="1"/>
Designator field for trunk (DES)	<input type="text"/>
Trunk Type (TKTP)	<input type="text" value="TIE"/>
Incoming and Outgoing trunk (ICOG)	<input type="text" value="Incoming and Outgoing (IAO)"/>
Access Code for the trunk route (ACOD)	<input type="text" value="555"/>
The route is for a virtual trunk route (VTRK)	<input type="checkbox"/>
Digital Trunk Route (DTRK)	<input type="checkbox"/>
Integrated Services Digital Network option (ISDN)	<input type="checkbox"/>

**+ Basic Route Options**

**+ Network Options**

**+ General Options**

**+ Advanced Configurations**

\* **Mandatory fields of current configuration**

### Basic Configuration

In the **Basic Configuration** section of this web page (see [Figure 83](#)), the following functions can be performed:

- Assign a **Route Number** (ROUT) using the drop-down list.
- Enter a **Designation** (DES) for the route.
- Select a **Trunk Type** (TKTP) from the drop-down list.
- Use the drop-down list to indicate that the trunk is **Incoming and/or Outgoing** (ICOG).
- Assign an **Access Code** (ACOD) to the trunk route.

Element Manager may request that users enter data for additional parameters, depending on what is entered in the Basic Configuration fields. Choices in the drop-down lists for every parameter in the Basic Configuration fields are determined by the data entered above that field.

**Figure 83**  
**Basic Configuration for routes**

- Basic Configuration	
Input Description	Input Value
Route Data Block (RDB) (TYPE)	RDB
Customer number (CUST)	00
Route Number (ROUT)	10
Designator field for trunk (DES)	ISDN V TRUNKS
Trunk Type (TKTP)	TIE
Incoming and Outgoing trunk (ICOG)	Incoming and Outgoing (AO)
Access Code for the trunk route (ACOD)	8110
The route is for a virtual trunk route (VTRK)	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE)	000 <span style="color: green;">Range: 0 - 255</span>
- Node ID of signaling server of this route (NODE)	8 <span style="color: green;">Range: 0 - 9999</span>
- Protocol ID for the route (PCID)	H323 (H323)
Integrated Services Digital Network option (ISDN)	<input checked="" type="checkbox"/>
- Mode of operation (MODE)	Route uses ISDN Signaling Link (SLD)
- D channel number (DCH)	10
- Interface type for route (IFC)	Meridian M1 (SL1)
- Private Network Identifier (PNI)	00002 <span style="color: green;">Range: 0 - 32700</span>
- Network Calling Name Allowed (NCNA)	<input checked="" type="checkbox"/>
- Network Call Redirection (NCRD)	<input checked="" type="checkbox"/>
- Trunk Route Optimization (TRO)	<input checked="" type="checkbox"/>
- Recognition of DT12 ABCD FALT signal for ISL (FALT)	<input type="checkbox"/>

To save changes made in this section, click **Submit** at the bottom of the **Route Property Configuration** web page.

### **Basic Route Options**

In the **Basic Route Options** section (see [Figure 84 on page 182](#)), use the check boxes to activate the following options for this route:

- Billing Number Required (BILN)
- Call Detail Recording (CDR)
- Controls or timers (CNTL)
- Conventional (TIE trunk only) (CNVT)
- Incoming DID Digit Conversion (IDC)
- Process Notification Networked Calls (PNNC)

In addition, use the drop-down list to select a Multi-frequency Compelled or MFC Signaling (MFC) type.

*Note:* The route used in this example is a TIE trunk route. The inputs requested by Element Manager vary depending on the responses to earlier input requests, including Trunk Type (TKTP).

Depending on which boxes are selected in the preceding list, Element Manager requests that users enter data for additional parameters, as shown in [Figure 84 on page 182](#).

**Figure 84**  
**Basic Route Options configuration**

Input Description	Input Value
<b>- Basic Route Options</b>	
- Billing Number Required (BLN)	<input checked="" type="checkbox"/>
- Billing Number Length (BLN)	10
- Billing number (BNUM)	<input type="text"/>
- Billing Number Displayed (BDSP)	<input type="checkbox"/>
<b>Call Detail Recording (CDR)</b>	
- CDR records generated on incoming calls (INC)	<input type="checkbox"/>
- CDR record printing content option for redirected calls (LAST)	<input type="checkbox"/>
- Time To Answer output in CDR (TTA)	<input checked="" type="checkbox"/>
- Abandoned call records output for this route (ABAN)	<input type="checkbox"/>
- Abandoned call on busy tone records (CDRB)	<input type="checkbox"/>
- CDR ACD O initial connection records to be generated (OREC)	<input type="checkbox"/>
- CDR on outgoing calls (OAL)	<input type="checkbox"/>
- North American Toll scheme (NATL)	<input checked="" type="checkbox"/>
<b>Controls or timers (CNTL)</b>	
- Trunk Timers (TIMR)	<input type="button" value="Edit"/>
- Seizure Supervision Timer in seconds (SST)	50
<b>- Dial Tone Detection (DTD)</b>	
- Extended Tone Detector Table Number (XTDT)	<input type="button" value="v"/>
- Minimum Dial Tone Detection delay in seconds (MDTD)	5

To save changes made in this section, click **Submit** at the bottom of the **Route Property Configuration** web page.

### Network Options

Figure 85 on page 183 provides an example of the input requested in the **Network Options** section for the route shown in Figure 82 on page 179. The actual input that Element Manager requests varies depending on the type of route and the responses to earlier input requests.

**Figure 85**  
**Network Options for routes**

- Network Options	
Input Description	Input Value
Electronic Switched Network pad control (ESN)	<input type="checkbox"/>
Signaling arrangement (SIGO)	Standard (STD)
Route Class (RCLS)	Route Class marked as external (EXT)
Off-Hook Queuing (OHO)	<input type="checkbox"/>
Off-Hook Queue Threshold (OHOT)	0
Call Back Queuing (CBO)	<input type="checkbox"/>
Number of Digits (NDIG)	2
Authcode (AUTH)	<input type="checkbox"/>

To save changes made in this section, click **Submit** at the bottom of the **Route Property Configuration** web page.

### General Options

Figure 86 provides an example of the input requested in the **General Options** section for the route shown in Figure 82 on page 179. The actual input that Element Manager requests varies depending on the type of route and the responses to earlier input requests.

**Figure 86**  
**General Options for routes**

- General Options	
Input Description	Input Value
Near End Disconnect Control (NEDC)	Originating end control (ORG)
Far End Disconnect Control (FEDC)	Originating end control (ORG)
M1 is the only Controlling Party on incoming calls (CPDC)	<input type="checkbox"/>
Dial Tone on originating calls (DLTN)	<input checked="" type="checkbox"/>
Hold failure threshold (HOLD)	02 02 40
Seize failure threshold (SEIZ)	02 02
Supervision Failure (SVFL)	02 02
Trunk Access Restriction Group (TARG)	01
Alternate trunk route for outgoing trunks (STEP)	Range: 0 - 511
Actual outgoing toll digits to be ignored for Code Restriction (OABS)	
Display IDC Name (DNAM)	<input type="checkbox"/>
Enable Equal Access Restrictions (EQAR)	<input type="checkbox"/>
ACD DNIS route (DNIS)	<input type="checkbox"/>
Include DNIS number in CDR records (DCDR)	<input type="checkbox"/>

To save changes made in this section, click **Submit** at the bottom of the **Route Property Configuration** web page.

### Advanced Configurations

Figure 87 provides an example of the input requested in the **Advanced Configurations** section for the route shown in Figure 82 on page 179. The actual input that Element Manager requests varies depending on the type of route and the responses to earlier input requests.

**Figure 87**  
Advanced Configurations for routes

- Advanced Configurations	
Input Description	Input Value
Malicious Call Trace Alarm is allowed for external calls (ALRM)	<input type="checkbox"/>
Allow last Re-directing Number (ARDN)	ARDN (NO) <input type="button" value="v"/>
ANI table Entry for Route (ANIE)	0 <span style="color: green;">Range: 0 - 511</span>
ANI identifier number (ANTK)	<input type="text"/>
AC 15 Timed Reminder Recall (ATRR)	<input type="checkbox"/>
Auto terminate (AUTO)	<input type="checkbox"/>
Block Transfer of Unanswered Call (BTUA)	<input type="checkbox"/>
CIS ANI Category Code (CAC_CIS)	3 <input type="button" value="v"/>
Collect Call Blocking Allowed (CCBA)	<input type="checkbox"/>
Call Forward Restriction (CFWR)	<input type="checkbox"/>
Maximum number of CNI digits (CLEN)	10 <input type="button" value="v"/>
Time (in seconds) that an extension is allowed to ring or be On-hold or Call Park before the trunk is disconnected (DCTI)	0 <span style="color: green;">Range: 0 - 511</span>
Default Model number (Option 11C) (DMOD)	<input type="button" value="v"/>
North American Distinctive Ringing for incoming calls (DRNG)	<input type="checkbox"/>
Facility Restriction Level (FRL)	<input type="text"/> <span style="color: green;">Range: 0 - 254</span>
Home Local Number (HLCL)	<input type="text"/>
Home National Number (HNTN)	<input type="text"/>
In-Band Automatic Number Identification route (IANI)	<input type="checkbox"/>

To save changes made in this section, click **Submit** at the bottom of the **Route Property Configuration** web page.

### New Trunk Configuration

Click the **Add Trunk** button beside a Customer Row or a Trunk Row to open the **New Trunk Configuration** web page for the selected customer, route, and trunk, as shown in Figure 88 on page 185.

**Figure 88**  
**New Trunk Configuration web page**

Managing: **192.167.100.3**  
 Routes and Trunks > [Routes and Trunks](#) > Customer 0, Route 1, New Trunk Configuration

### Customer 0, Route 1, New Trunk Configuration

**- Basic Configuration**

Input Description	Input Value
Multiple trunk input number (MTINPUT)	<input type="text"/>
Trunk data block (TYPE)	TIE trunk data block (TIE) <input type="text"/>
Terminal Number (TN)	<input type="text"/>
Designator field for trunk (DES)	<input type="text"/>
Extended Trunk (XTRK)	<input type="text"/>
Customer number (CUST)	<input type="text"/>
Route number, Member number (RTMB)	<input type="text"/>
Level 3 Signaling (SIGL)	<input type="text"/>
Card Density (CDEN)	<input type="text"/>
Start arrangement Incoming (STR)	<input type="text"/>
Start arrangement Outgoing (STRO)	<input type="text"/>
Trunk Group Access Restriction (TGAR)	<input type="text"/>
Channel ID for this trunk. (CHID)	<input type="text"/>
Increase or decrease the member numbers (INC)	Increase channel and member number (YES) <input type="text"/>
Class of Service (CLS)	<input type="button" value="Edit"/>

**+ Advanced Trunk Configurations**

The **New Trunk Configuration** web pages are divided into two categories:

- 1 Basic Configuration
- 2 Advanced Trunk Configurations

### Basic Configuration

In the **Basic Configuration** section of these web pages (see [Figure 88](#)), users can perform the following tasks:

- Enter a **Designator field (DES)** for the trunk.
- Select an **Extended Trunk (XTRK)** card type from the drop-down list.
- Edit the route or member number in the **Route number, Member number (RTMB)** text box. The range is 0-4000.
- Use the **Level 3 Signaling (SIGL)** drop-down list to select a Level 3 signaling method.

- Use the **Start arrangement Incoming (STRI)** drop-down list to select a start arrangement for incoming calls.
- Use the **Start arrangement Outgoing (STRO)** drop-down list to select a start arrangement for outgoing calls.
- Use the **Increase or decrease the member numbers (INC)** drop-down list to select either increasing channel numbers and member numbers or increasing channel numbers and decreasing member numbers.
- Click the **Class of Service (CLS) Edit** button to view Class of Service information for the trunk. See [Figure 89](#).

**Figure 89**  
**Class of Service Configuration web page**

Managing: [192.167.100.3](#)  
 Routes and Trunks > Routes and Trunks > Customer 0, Route 1, New Trunk Configuration > Class of Service Configuration

### Class of Service Configuration

**- Class of Service**

Input Description	Input Value
- ACD Priority (CLS)	<input type="text"/>
- Barring (CLS)	<input type="text"/>
- Calling Line Identification (CLS)	<input type="text"/>
- Calling party (CLS)	<input type="text"/>
- Central Office Ringback (CLS)	<input type="text"/>
- Dial Pulse (CLS)	<input type="text"/>
- DTR PAD value (CLS)	<input type="text"/>
- Echo Canceling (CLS)	<input type="text"/>
- Hong Kong DTI (CLS)	<input type="text"/>
- Priority (CLS)	<input type="text"/>
- Manual Incoming (CLS)	<input type="text"/>
- Make-break ratio for dial pulse (CLS)	<input type="text"/>
- Polarity (CLS)	<input type="text"/>
- Short or long line (CLS)	<input type="text"/>
- Analog Semi-Permanent Connections (CLS)	<input type="text"/>
- Centrex Switchhook Flash (CLS)	<input type="text"/>

*Note:* The member used in this example is a TIE trunk. The inputs requested by Element Manager may vary depending on the responses to earlier input requests.

To save changes made in this section, click **Submit** at the bottom of the **New Member Configuration** web page.

## Advanced Trunk Configurations

Figure 90 provides an example of the input requested in the **Advanced Trunk Configurations** section for the TIE Trunk shown in Figure 88 on page 185.

**Figure 90**  
Advanced Configurations for trunks

Advanced Trunk Configurations	
Input Description	Input Value
CTI trunk Monitoring and Control (AST)	<input type="checkbox"/>
Auto Terminate DN (ATDN)	<input type="text"/>
Music Conference Loop (CLP)	<input type="text"/> Range: 0 - 159
Call Modification Features restriction (CMF)	<input type="checkbox"/>
Digit Collection Ready (DTCR)	<input type="checkbox"/>
Forced Charge Account (FCAR)	<input type="checkbox"/>
Multifrequency PAD (MFDP)	<input type="checkbox"/>
Manual Directory Number (MNDN)	<input type="text"/>
Network Class of Service group (NCOS)	0
Night Service Group number (NGRP)	0
Night Service directory number (NITE)	<input type="text"/>
Pulse Code Modulation Law (PCML)	<input type="text"/>
Pad Category table number for digital trunks (PDCA)	1
Private Line Directory Number (PRDN)	<input type="text"/>
Is the ISPC link used by a D-channel (SDCH)	<input type="checkbox"/>
Signaling Category table number (SICA)	1
Connection Reference Number (SREF)	<input type="text"/> Range: 1 - 9999999
Answer and disconnect Supervision required (SUPN)	<input type="checkbox"/>
Step-by-step CO trunk (SXS)	<input type="checkbox"/>
Trunk Identifier (TKID)	<input type="text"/>

**Note:** The member used in this example is a TIE trunk. The inputs requested by Element Manager may vary depending on the responses to earlier input requests.

To save changes made in this section, click **Submit** at the bottom of the web page.

### Delete multiple trunk members

Click **Multi-Del** located beside a member row to open the **Delete multiple trunk members** web page for the selected member, as shown in Figure 91 on page 188. On this web page, the information for the Parent Route is read-only.

**Figure 91**  
Delete multiple trunk members page

Managing: **192.167.100.3**  
Routes and Trunks > [Routes and Trunks](#) > Customer 0, Route 1, Delete multiple trunk members

---

**Customer 0, Route 1, Delete multiple trunk members**

**Parent Route Information**

Input Description	Input Value
Customer number (CUST_NUM)	0
Route number (ROUT_NUM)	1
Route description (ROUT_DES)	NONE
Trunk type (TKTP)	TIE
Total trunk members (TOTL_TN)	2

**Select TN and deleting number**

Selection Description	Selection Value
Set starting TN number to be deleted (OUT)	Trunk: 1; TN: 004 0 04 01
Set total trunk number to be deleted (up to 32)	1

To delete multiple trunk members using this web page:

- 1 Use the **Set starting TN to be deleted** drop-down list to determine the start of the deletion list.
- 2 Use the **Set total trunk number to be deleted** drop-down list to indicate the total number of trunks to be deleted (up to 32).
- 3 Click **Delete**.

## D-channels

Click the **D-Channels** link on the **Routes and Trunks** branch of the Element Manager navigator to open the **D-Channels** web page. This web page allows users to configure or edit D-channel information, as shown in [Figure 92 on page 189](#).

**Figure 92**  
**D-Channels web page**

Managing: [192.167.100.3](#)  
Routes and Trunks » D-Channels

---

## D-Channels

**Maintenance**

[D-Channel Diagnostics \(LD 96\)](#)  
[Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)  
[MSDL Diagnostics \(LD 96\)](#)  
[TMDI Diagnostics \(LD 96\)](#)  
[D-Channel Expansion Diagnostics \(LD 48\)](#)

**Configuration**

Choose a D-Channel Number:  and type:

- Channel: 0	Type: DCH	Card Type: DCHI	Description:	<input type="button" value="Edit"/>
--------------	-----------	-----------------	--------------	-------------------------------------

### Maintenance

This sections contains links to the following commands:

- D-Channel Diagnostics (LD 96)
- Network and Peripheral Equipment (LD 32, Virtual D-Channels)
- MSDL Diagnostics (LD 96)
- TMDI Diagnostics (LD 96)
- D-Channel Expansion Diagnostics (LD 48)

For more information on these commands, see “System” on [page 39](#).

### Configuration

From the **D-Channels** web page users can view basic information on existing D-channels.

This web page also contains buttons that link to additional web pages. Follow these links to do the following:

- add a new D-channel
- edit D-channel data

To add a new D-channel, select a number from the **Choose a D-channel Number** drop-down list, select a D-channel type from the **type** drop-down list, and click to **Add**. To edit the configuration information on an existing D-channel, click the **Edit** button located to the right of the Description field.

Click the **to Add** button, or any of the **Edit** buttons, to open the **D-Channels Property Configuration** web page for that channel, as shown in [Figure 93](#)).

*Note:* H.323 and SIP can use the same D-channel.

**Figure 93**  
**D-Channels Property Configuration web page**

Managing: [192.167.100.3](#)  
Routes and Trunks > D-Channels > D-Channels 1 Property Configuration

### D-Channels 1 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Action Device And Number (ADAN) (TYPE)	DCH
D channel Card Type (CTYP)	<input type="text"/>
Group number (GRP)	<input type="text"/>
Device number (DNUM)	<input type="text"/>
Port number (PORT)	<input type="text"/>
Designator (DES)	<input type="text"/>
Recovery to Primary (RCVP)	<input type="checkbox"/>
User (USR)	<input type="text"/>
Interface type for D-channel (IFC)	Meridian DMS-100 (D100)
Country (CNTY)	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number (DCHL)	<input type="text"/>
Primary Rate Interface (PRI)	<input type="text"/> <input type="button" value="more PRI"/>
Secondary PRI2 loops (PRI2)	<input type="text"/>
Meridian 1 node type (SIDE)	Slave to the controller (USR)
Release ID of the switch at the far end (RLS)	25
Central Office switch type (CO_TYPE)	100% compatible with Bellcore standard (STD)

In the **D-Channels Property Configuration** web page, users can:

- Enter information on the **Basic Configuration** web page.
  - The information entered in this section corresponds to ADAN and ADAN DCH (Action Device and Number, D-channel and back-up D-channels) data traditionally configured using LD 17 - Configuration Record 1. In addition to basic D-channel configuration, additional information can be entered for optional settings in the following two categories:
    - Basic D-channel options (BSCOPT)
    - Advanced D-channel options (ADVOPT)

These options are shown in [Figure 94](#).

**Figure 94**  
**Basic and Advanced D-Channel options**

**- Basic options (BSCOPT)**

- Primary D-channel for a backup DCH (PDCH)
- PINK customer number (PINK\_CUST)
- Progress signal (PROG)
- Calling Line Identification (CLID)
- Output request Buffers (OTBF)
- D-channel transmission Rate (DRAT)
- Channel Negotiation option (CNEG)
- Remote Capabilities (RCAP)

**+ - Change protocol timer value (TIMR)**

- B channel Service messaging. (BSRV)

**- Advanced options (ADVOPT)**

- Layer 3 call control message count per 5 second time interval (ISDN\_MCNT)  Range: 60 - 350
- Number of Status Enquiry Messages sent within 128 ms (SEMT)
- Map channel number to timeslots on a PRI2 loop (QCHID)

**+ H323 Overlap Signaling Settings (H323)**

- Overlap Timer (OVLTI)
- Multilocation Business Group Allowed (MBGA)
- Network Attendant Service Allowed (NASA)

**+ - Link Access Protocol for D-channel (LAPD)**

**+ Feature Packages**

- Configure information on the **Feature Packages** web page.

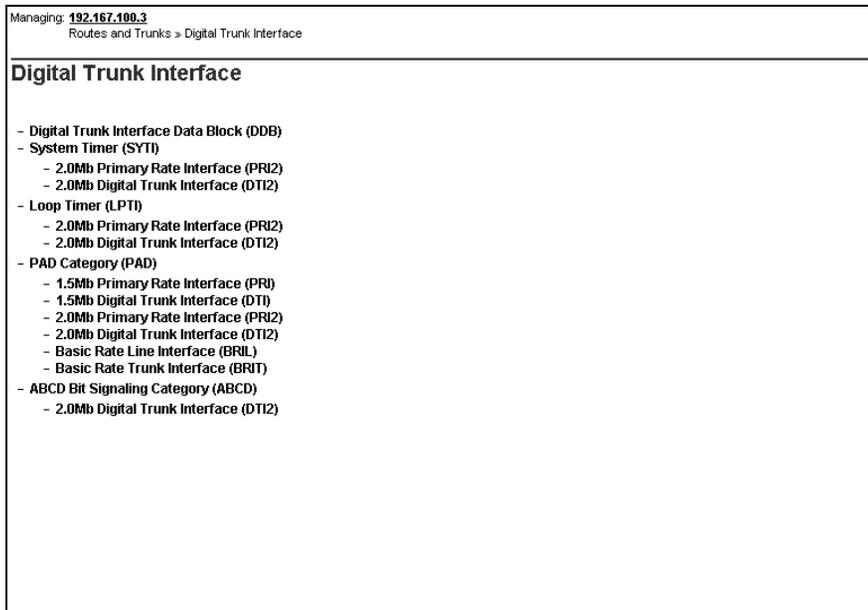
- Digital Private Networking Signaling System 1 (Package 123)
- Virtual Network Services (Package 183)

To save changes made in this section, click **Submit** at the bottom of the **D-channels Property Configuration** web page.

## Digital Trunk Interface

When the user clicks the **Digital Trunk Interface** link on the **Routes and Trunks** branch of the Element Manager navigator, the **Digital Trunk Interface** web page opens, as shown in [Figure 95](#). This web page allows the user to configure or edit Digital Trunk Interface information.

**Figure 95**  
**Digital Trunk Interface web page**



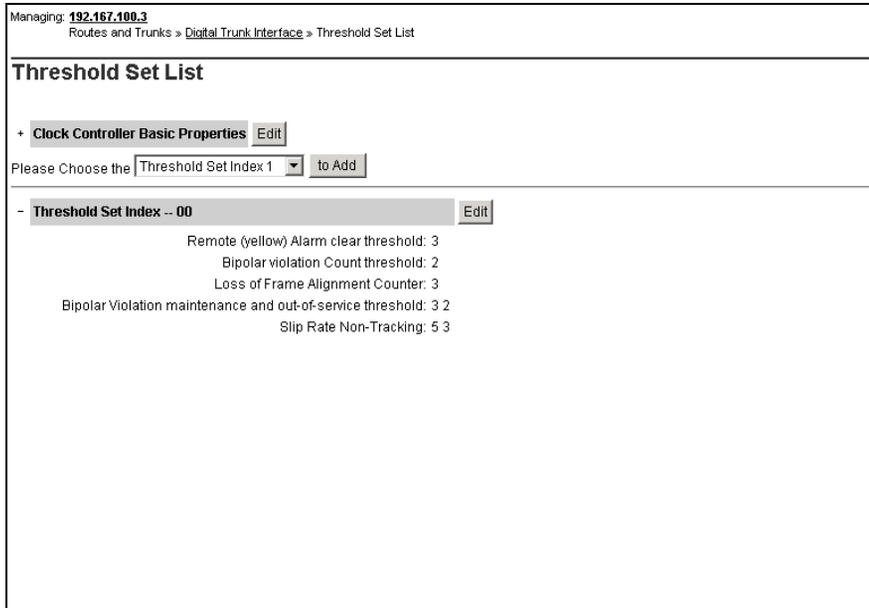
From this web page, users can access additional web pages to perform the following functions:

- configure Digital Trunk Interface Data Block (DDB) information

- configure System Timer (SYSTI) parameters for:
  - 2.0 Mb Primary Rate Interface (PRI2)
  - 2.0 Mb Digital Trunk Interface (DTI2)
- configure Loop Timer (LPTI) parameters for:
  - 2.0 Mb Primary Rate Interface (PRI2)
  - 2.0 Mb Digital Trunk Interface (DTI2)
- configure PAD Category (PAD) parameters for:
  - 1.5 Mb Primary Rate Interface (PRI)
  - 1.5 Mb Digital Trunk Interface (DTI)
  - 2.0 Mb Primary Rate Interface (PRI2)
  - 2.0 Mb Digital Trunk Interface (DTI2)
  - Basic Rate Line Interface (BRIL)
  - Basic Rate Trunk Interface (BRIT)
- configure ABCD Bit Signaling Category (ABCD) parameters for the 2.0 Mb Digital Trunk Interface (DTI2)

To configure or edit Digital Trunk Interface Data Block (DDB) information, click **Digital Trunk Interface Data Block (DDB)**. The **Threshold Set List** web page opens. See [Figure 96 on page 194](#).

**Figure 96**  
**Threshold Set List web page**



From this web page, users can access additional web pages to perform the following functions:

- edit Clock Controller Basic Properties
- add a Threshold Set Index
- edit an existing Threshold Set Block

Users can edit Clock Controller properties by clicking the **Edit** button next to the **Clock Controller Basic Properties** button. The **Clock Controller Basic Properties** web page opens, as shown in [Figure 97 on page 195](#).

**Figure 97**  
**Clock Controller Basic Properties web page**

Managing: 192.167.100.3  
 Routes and Trunks > Digital Trunk Interface > Threshold Set List > Clock Controller Basic Properties

### Clock Controller Basic Properties

Input Description	Input Value
Card number for Clock Controller (Option 11C) (CC0):	<input type="text"/>
- Primary Reference (PREF_CC0):	<input type="text"/>
- Secondary Reference (SREF_CC0):	<input type="text"/>
Card number for Clock Controller (Option 11C) (CC1):	<input type="text"/>
- Primary Reference (PREF_CC1):	<input type="text"/>
- Secondary Reference (SREF_CC1):	<input type="text"/>
Card number for Clock Controller (Option 11C) (CC2):	<input type="text"/>
- Primary Reference (PREF_CC2):	<input type="text"/>
- Secondary Reference (SREF_CC2):	<input type="text"/>
Card number for Clock Controller (Option 11C) (CC3):	<input type="text"/>
- Primary Reference (PREF_CC3):	<input type="text"/>
- Secondary Reference (SREF_CC3):	<input type="text"/>
Card number for Clock Controller (Option 11C) (CC4):	<input type="text"/>
- Primary Reference (PREF_CC4):	<input type="text"/>
- Secondary Reference (SREF_CC4):	<input type="text"/>
Multi Purpose Serial Data Link Idle Code Selection (ICS):	<input type="text"/>

Users can then enter the required information in the text boxes.

To add or edit a Threshold Set Index, follow the steps in Procedure 6.

#### **Procedure 6** **Adding or editing a Threshold Set Index**

To add a Threshold Set Index

- 1** Select a **Threshold Set Index** from the drop-down list.
- 2** Click to **Add**.

To edit the configuration information in an existing Threshold Set Block, click **Edit** located to the right of the index number.

————— **End of Procedure** —————

When the **to Add** button or a Threshold Set Index Edit button is clicked on [Figure 96 on page 194](#), the **Threshold Set Block** web page for that index opens, as shown in [Figure 98](#).

**Figure 98**  
**Threshold Set Block web page**

Managing: 192.167.100.3  
Routes and Trunks > Digital Trunk Interface > Threshold Set List > Threshold Set Block

### Threshold Set Block

Input Description	Input Value
Threshold set (TRSH):	<input type="text" value="00"/>
Remote (yellow) Alarm clear threshold (RALM):	<input type="text" value="3"/>
Bipolar violation Count threshold (BIPC):	<input type="text" value="2"/>
Loss of Frame Alignment Counter (LFAC):	<input type="text" value="3"/>
Bipolar Violation maintenance and out-of-service threshold (BIPV):	<input type="text" value="3"/> <input type="text" value="2"/>
Slip Rate Tracking mode maintenance (SRTK):	<input type="text" value="5"/> <input type="text" value="30"/>
Slip Rate Non-Tracking (SRNT):	<input type="text" value="5"/> <input type="text" value="3"/>
Loss of Frame Alignment maintenance and out-of-service thresholds (LFAL):	<input type="text" value="17"/> <input type="text" value="511"/>
Slip Rate Improvement Monitoring time in minutes (SRIM):	<input type="text" value="1"/>
Slip Rate Maintenance Maximum (SRMM):	<input type="text" value="2"/>

The information entered in this section corresponds to DDB (Digital Trunk Interface Data Block) information traditionally configured using LD 73 - Digital Trunk Interface.

To save changes made in this section, click **Submit** at the bottom of the **Threshold Set Block** web page.

---

# Dialing and Numbering Plans

---

## Contents

This section contains information on the following topics:

Introduction . . . . .	197
Electronic Switched Network . . . . .	198
Network Control & Services . . . . .	199
Coordinated Dialing Plan . . . . .	199
Numbering Plan . . . . .	200
Network Routing Service and NRS Manager . . . . .	200
Access levels . . . . .	204
Flexible Code Restriction . . . . .	206
Incoming Digit Conversion . . . . .	209

## Introduction

Element Manager enables users to configure the Dialing and Numbering Plans for the Call Server and the Network Routing Service (NRS) Manager. The information configured in the Dialing and Numbering Plans corresponds to the Command Line Interface (CLI) prompts and responses for Electronic Switched Network (ESN) data traditionally configured in LD 86, LD 87, and LD 90.

For more information on the overlays referred to in this chapter, see *Software Input/Output: Administration* (553-3001-311) and *Software Input/Output: Maintenance* (553-3001-511).

## Electronic Switched Network

To configure or edit the Dialing and Numbering Plan for the Electronic Switched Network, click the **Electronic Switched Network** link in the **Dialing and Numbering Plans** branch of the Element Manager navigator. The **Electronic Switched Network (ESN)** web page opens, as shown in [Figure 99](#). From this web page users can configure the Dialing and Numbering Plan for each customer on the Electronic Switched Network.

Element Manager provides access to the following Dialing and Numbering Plan parameters:

- Network Control & Services
- Coordinated Dialing Plan (CDP)
- Numbering Plan (NET)

**Figure 99**  
**Electronic Switched Network (ESN) web page**

Managing: [192.167.100.3](#)  
Dialing and Numbering Plans > Electronic Switched Network (ESN)

---

### Electronic Switched Network (ESN)

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - ESN Access Codes and Parameters (ESN)
    - Digit Manipulation Block (DGT)
    - Route List Block (RLB)
    - Incoming Trunk Group Exclusion (ITGE)
    - Network Attendant Services (NAS)
  - Coordinated Dialing Plan (CDP)
    - Local Steering Code (LSC)
    - Distant Steering Code (DSC)
    - Trunk Steering Code (TSC)
  - Numbering Plan (NET)
    - Access Code 1
      - Home Area Code (HNPA)
      - Home Location Code (HLOC)
      - Location Code (LOC)
      - Numbering Plan Area Code (NPA)
      - Exchange (Central Office) Code (NXX)
      - Special Number (SPN)
      - Network Speed Call Access Code (NSCL)
      - Free Calling Area Screening (FCAS)
      - Free Special Number Screening (FSNS)
    - Access Code 2
      - Home Area Code (HNPA)
      - Home Location Code (HLOC)
      - Location Code (LOC)
      - Numbering Plan Area Code (NPA)
      - Exchange (Central Office) Code (NXX)

## Network Control & Services

Under Network Control & Services, users can click the links to configure or modify the parameters associated with the following items:

- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)

The Network Control Parameters (NCTL) that are configurable using Element Manager correspond to data traditionally configured in LD 87. The settings for the remaining five items under Network Control & Services correspond to CLI prompts and responses in LD 86.

The total free and used Location Codes (LOCs) are displayed at the **Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer xx > Network Control & Services > ESN Access Codes and Basic Parameters** web page.

This feature has its own packaging (LOCX). The package must be added under **Customers > Customer xx Property Configuration > Feature Packages**. This package can be activated only when the FNP package is enabled.

## Coordinated Dialing Plan

Under Coordinated Dialing Plan (CDP), users can click links to configure or modify parameters associated with the following codes:

- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)

The Coordinated Dialing Plan parameters that are configurable using Element Manager correspond to data traditionally configured in LD 87.

## Numbering Plan

Under Numbering Plan (NET), users can click links to configure or modify parameters associated with the following codes:

- Home Area Code (HNPA)
- Home Location Code (HLOC)
- Location Code (LOC). Maximum number of LOCs is 16 000.
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)

These codes can also be configured using the prompts and responses in LD 90.

Numbering Plan (NET) is also used to configure the following two LD 87 features:

- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)

## Network Routing Service and NRS Manager

The Network Routing Service (NRS) is a web-based application that runs on the Signaling Server. The purpose of the NRS is as follows:

- It populates the location and registration database.
- It adds the appearance of the proxy in the customer network.
- It facilitates a translation database, for phone numbers contained within the SIP Uniform Request Identifier (URI) in order to present a well formed, syntactically correct, phone number to the location service within the proxy.

For more information on NRS and NRS Manager, see *IP Peer Networking: Installation and Configuration* (553-3001-213).

All CS 1000S or CS 1000M systems in the network are registered with the NRS. The NRS runs on an Enterprise Translations Server and provides routing services to several service provider networks. The hierarchy consists of:

- Service Domain — represents a service provider network
- Level 1 Domain (User Data Protocol) — represents a sub-domain in a service domain, and is referred to as the L1-domain
- Level 0 Domain (Coordinated Dialing Plan) — represents a sub-domain in an L-1 domain, and is referred to as the L0-domain.
- Gateway Endpoint — represents a gateway, and exists within an L0-domain.
- User Endpoint — represents a SIP Phone. It exists with the L0 domain. A site can have many SIP Phones.
- Routing Entry — represents a range of addresses that a gateway can terminate calls to, and exists within a gateway.
- Collaborative Server — a server in another network zone that can be used to resolve requests when the NRS cannot find a match in its numbering plan database.

For redundancy purposes, the NRS translation servers can be organized into hierarchical clusters.

The NRS handles a centralized numbering plan for the network. This enables simplified management of the network. The NRS supports H.323, SIP, and Network Connection Server (NCS) protocols. The NRS can provide NRS features to other H.323- and SIP-compliant endpoints (for example, CS 1000S and IP Trunk 4.0 endpoints).

NRS Manager must be running Microsoft™ Internet Explorer 6.00 or later. Netscape Navigator is not supported. Click the **Network Routing Service** link in the **Dialing and Numbering Plans** branch of the Element Manager navigator to access the NRS Manager as shown in [Figure 100 on page 202](#). The format of the NRS URL is `http://<NRSM_server_IP_address>/nrs`.

**Figure 100**  
**Network Routing Service (NRS) configuration web page**

Managing: **192.167.100.3**  
Dialing and Numbering Plans > Network Routing Service (NRS)

### Network Routing Service (NRS)

Please enter the NRS IP Address then press button "Next >"

Input description	Input value
NRS IP Address:	192.167.101.2

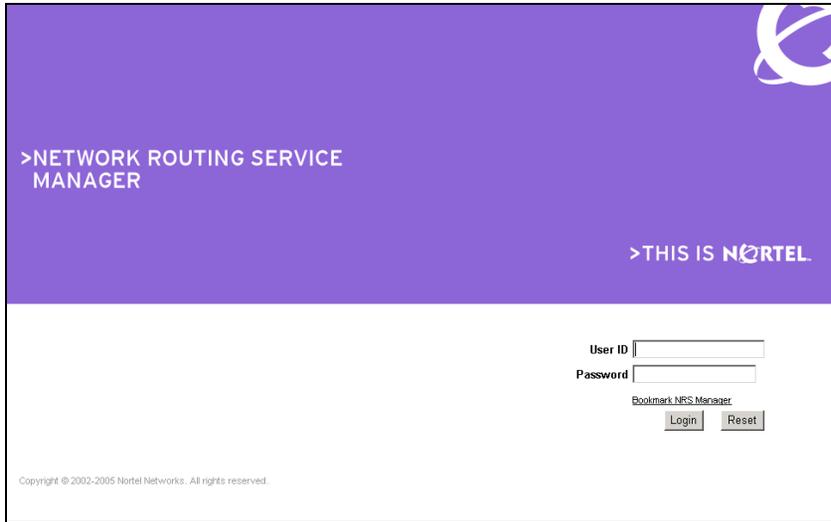
Next >

An alternate way to connect to the NRS is to enter the NRS IP address followed by */nrs* as a URL from any web browser on the network. For example, enter <http://47.11.249.84/nrs>.

Specifying the complete URL and including *nrs* is important. The NRS can be co-resident with other applications running on the Signaling Server platform. If other Signaling Server applications (for example, Terminal Proxy Server) also use a web-based management tool, then those management tools can use the URL <http://47.11.249.84/tps>.

The **Network Routing Service Manager login** web page opens (see [Figure 101 on page 203](#)). Enter the user name and password and click **Login**.

**Figure 101**  
**NRS Manager login web page**



The **NRS Home** web page opens (see [Figure 102 on page 204](#)).

**Figure 102**  
NRS Home web page

The screenshot shows the NRS Home web page. On the left is a navigation menu with links: => NRS Overview, System Wide Settings, and NRS Server Settings. The main content area has a breadcrumb 'Location: Home > NRS Overview >'. Below this is a section titled 'Network Routing Service' with the following details:

Software version	sse-4.30.20
Connected NRS role	PrimaryNRS
Primary NRS IP (TLAN)	192.168.253.6
Primary NRS state	ACTIVE
Alternate NRS IP (TLAN)	Unknown
Alternate NRS state	Unknown
Alternate permanent in service	OFF

Below this is a section titled 'Configured Components' with the following statistics:

# of Service Domains	0
# of L1 Domains (UDP)	0
# of L0 Domains (CDP)	0
# of Gateway Endpoints	0
# of User Endpoints	0
# of Routing Entries	0
# of Default Routes	0
# of Collaborative Servers	0

At the bottom is a section titled 'Users Logged Into This NRS Manager' with one entry:

admin	207.179.154.209
-------	-----------------

## Access levels

NRS Manager provides two levels of access:

- 1 **Monitor access.** Enables the user to view configuration data and view the output from performance monitoring functions. The user cannot modify any NRS configurations or settings, including monitor login user name and password.
- 2 **Administrator access.** Enables full administrative access to the NRS Manager. All configuration entries can be updated and full write access is given to the database, including the ability to change all system passwords.

When logging in using Administrator access, NRS opens with the web page shown in [Figure 102](#).

**Monitor access**

When accessing the NRS Manager as a monitor, users can view configuration data and reports from the performance monitoring functions.

**Administrator access**

To make changes to the NRS configuration, log into the NRS Manager using administrator access. In addition to the monitoring functionality available with Guest access, administrators can access configuration and administration functions.

Use the NRS Manager to:

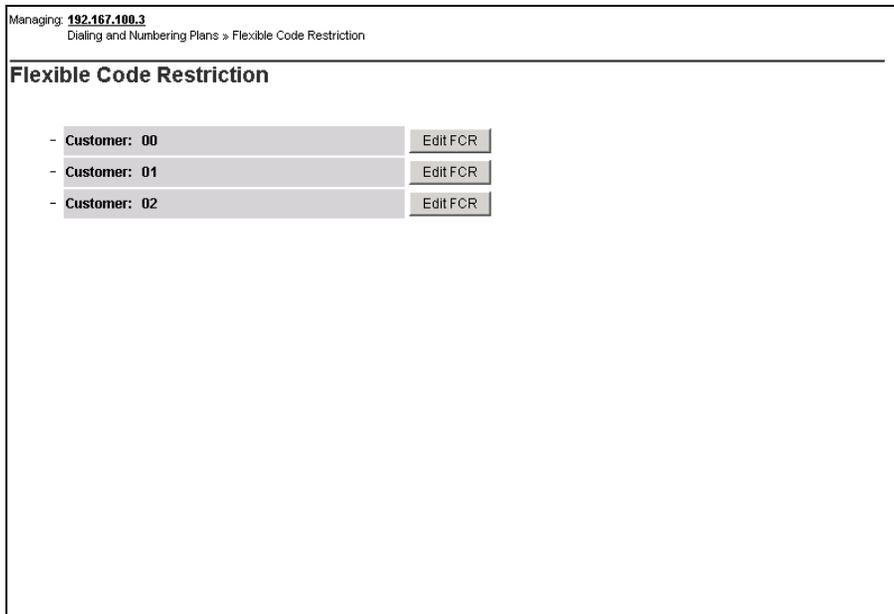
- configure system-wide settings
- configure NRS server settings
- provision Network Numbering Plans (Service Domains, L1 Domains, L0 Domains, Gateway Endpoints, routing entries, default routes, and collaborative servers)
- test Numbering Plans
- perform NRS server actions
- perform database actions
- perform Gatekeeper/NRS data conversion
- perform SIP phone context mapping
- view database sync and database status reports
- configure users

For detailed information on performing these procedures and managing the NRS using Element Manager, see *IP Peer Networking: Installation and Configuration* (553-3001-213).

## Flexible Code Restriction

To configure or edit Flexible Code Restriction information, click the **Flexible Code Restriction** link in the **Dialing and Numbering Plans** branch of the Element Manager navigator. The **Flexible Code Restriction** web page opens, as shown in [Figure 103](#).

**Figure 103**  
**Flexible Code Restriction web page**



This web page contains **Edit FCR** buttons that link to **Flexible Code Restriction Property** web pages for each of the customers configured on the Call Server.

To view the list of Flexible Code Restriction Trees for a customer, click the **Edit FCR** button located beside the customer number. The **Flexible Code Restriction Property** web page for the selected customer opens (see [Figure 104 on page 207](#)).

**Figure 104**  
**Flexible Code Restriction Property web page**

Managing: [192.167.100.3](#)  
Dialing and Numbering Plans > [Flexible Code Restriction](#) > Customer 00 Flexible Code Restriction Property

### Customer 00 Flexible Code Restriction Property

- Code Restriction Tree Number: 0	Edit CRNO
- Code Restriction Tree Number: 1	New CRNO
- Code Restriction Tree Number: 2	New CRNO
- Code Restriction Tree Number: 3	New CRNO
- Code Restriction Tree Number: 4	New CRNO
- Code Restriction Tree Number: 5	New CRNO
- Code Restriction Tree Number: 6	New CRNO
- Code Restriction Tree Number: 7	New CRNO
- Code Restriction Tree Number: 8	New CRNO
- Code Restriction Tree Number: 9	New CRNO
- Code Restriction Tree Number: 10	New CRNO
Code Restriction Tree Number: 11	New CRNO
Code Restriction Tree Number: 12	New CRNO
Code Restriction Tree Number: 13	New CRNO
Code Restriction Tree Number: 14	New CRNO
- Code Restriction Tree Number: 15	New CRNO

The **Flexible Code Restriction Property** web page contains buttons that link to Code Restriction Tree Configuration web pages for each Code Restriction Tree Number (CRNO). If there is an existing configuration for the CRNO, the button is labeled **Edit CRNO**. If a configuration has not been defined for the CRNO, the button is labeled **New CRNO**. Click the **Edit CRNO/New CRNO** button to open the **Code Restriction Tree Configuration** web page for the corresponding CRNO, as shown in [Figure 105 on page 208](#).

**Figure 105**  
**Code Restriction Tree Configuration web page**

Managing: **192.167.100.3**  
 Dialing and Numbering Plans > Flexible Code Restriction > Customer 00 Flexible Code Restriction Property > Code Restriction Tree 0 Configuration

---

**Code Restriction Tree 0 Configuration**

**- Code Restriction Tree Number Configuration**

Input Description	Input Value
Code Restriction Tree Number (CRNO)	<input type="text" value="0"/>
Initial - Allow or deny all codes. (INIT)	<input type="text" value="ALLOW"/>
<b>Digit sequence to be denied. (DENY)</b>	
<input type="text" value="1"/>	
Create new DENY <input type="text" value="1"/> Starting from <input type="text"/>	<input type="button" value="Add New"/>
<b>Digit sequence to be allowed. (ALLOW)</b>	
Create new ALLOW <input type="text" value="1"/> Starting from <input type="text"/>	<input type="button" value="Add New"/>
<b>Digit sequence to be bypassed. (BYPAS)</b>	
Create new BYPAS <input type="text" value="1"/> Starting from <input type="text"/>	<input type="button" value="Add New"/>

By entering values in the appropriate text boxes, users can:

- add or edit digit sequences to be enabled
- add or edit digit sequences to be denied

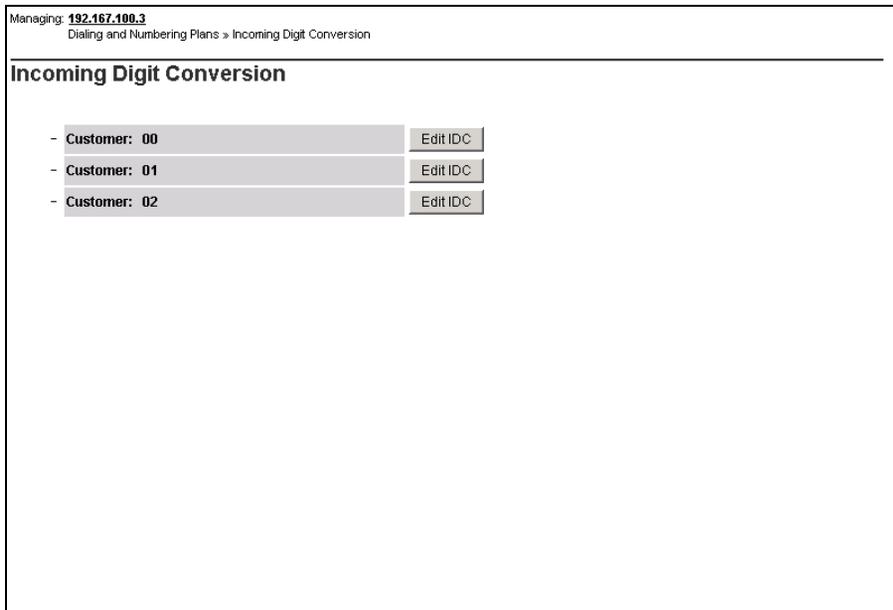
The information entered in this section corresponds to data traditionally configured using LD 49 - Flexible Code Restriction and Incoming Digit Conversion.

To save changes made in the configuration for this Code Restriction Tree, click **Submit** at the bottom of the web page.

## Incoming Digit Conversion

To configure or edit Incoming Digit Conversion information, click the **Incoming Digit Conversion** link in the **Dialing and Numbering Plans** branch of the Element Manager navigator. The **Incoming Digit Conversion** web page opens, as shown in [Figure 106](#).

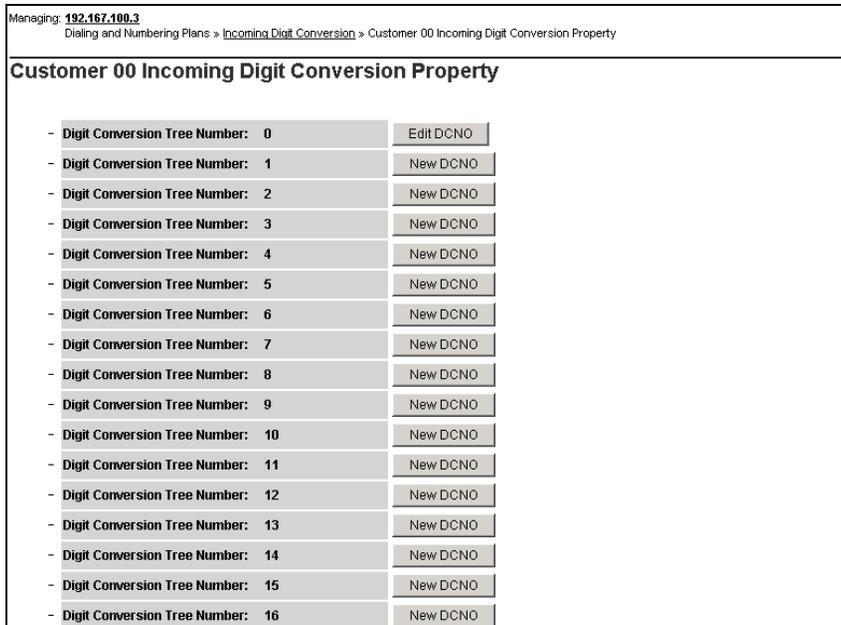
**Figure 106**  
**Incoming Digit Conversion web page**



This web page contains **Edit IDC** buttons that link to **Incoming Digit Conversion Property** web pages for each of the customers configured on the Call Server.

To view the list of Incoming Digit Conversion Trees for a customer, click the **Edit IDC** button located beside the customer number. The **Incoming Digit Conversion Property** web page for the selected customer opens. See [Figure 107 on page 210](#).

**Figure 107**  
**Incoming Digit Conversion Property web page**



The **Incoming Digit Conversion Property** web page contains buttons that link to **Digit Conversion Tree Configuration** web pages for each Digit Conversion Tree Number (DCNO). If there is an existing configuration for the DCNO, the button is labeled **Edit DCNO**. If a configuration has not been defined for the DCNO, the button is labeled **New DCNO**. Click the **Edit DCNO/New DCNO** button to open the **Digit Conversion Tree Configuration** web page for the corresponding DCNO. From this web page, users can configure Incoming Digit Conversion data.

**Figure 108**  
**Digit Conversion Tree Configuration web page**

Managing: 192.167.100.3  
 Dialing and Numbering Plans > Incoming Digit Conversion > Customer 00 Incoming Digit Conversion Property > Digit Conversion Tree 0 Configuration

### Digit Conversion Tree 0 Configuration

**- Digit Conversion Tree Number Configuration**

Input Description	Input Value
Digit Conversion Tree Number (DCNO)	0
Send calling party DID (SDID)	NO

**- Incoming Digits (IDGT)**

Incoming Digits	Converted Digits
Create new IDGT 1 <input type="button" value="Add New"/>	Starting from <input type="text"/>

The information entered in this section corresponds to data traditionally configured using LD 49 - Flexible Code Restriction and Incoming Digit Conversion.

To save changes made in the configuration for this Digit Conversion Tree, click **Submit** at the bottom of the web page.



---

# Services

---

## Contents

This section contains information on the following topics:

<a href="#">Introduction</a> . . . . .	213
<a href="#">Backup and Restore</a> . . . . .	213
<a href="#">Date and Time</a> . . . . .	223
<a href="#">Logs and Reports</a> . . . . .	225

## Introduction

The following Call Server Services can be accessed through Element Manager running on a Small System:

- Backup and Restore
- Date and Time
- Logs and Reports

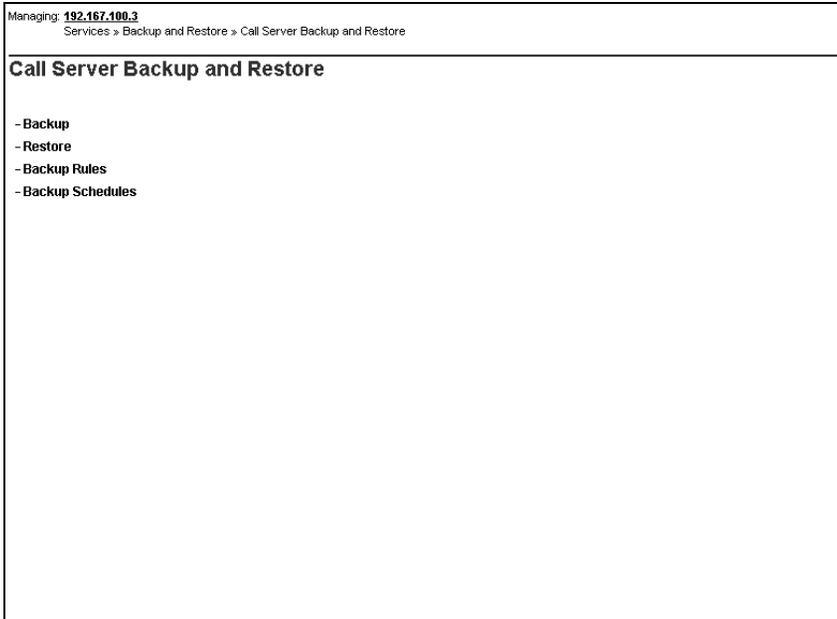
## Backup and Restore

The **Backup and Restore** link of the **Services** branch of the Element Manager navigator provides access to Call Server Backup and Restore functions.

## Call Server

In the **Services** branch of the Element Manager navigator, click **Backup and Restore > Call Server**. The **Call Server Backup and Restore** web page opens (see [Figure 109](#)).

**Figure 109**  
**Call Server Backup and Restore web page**

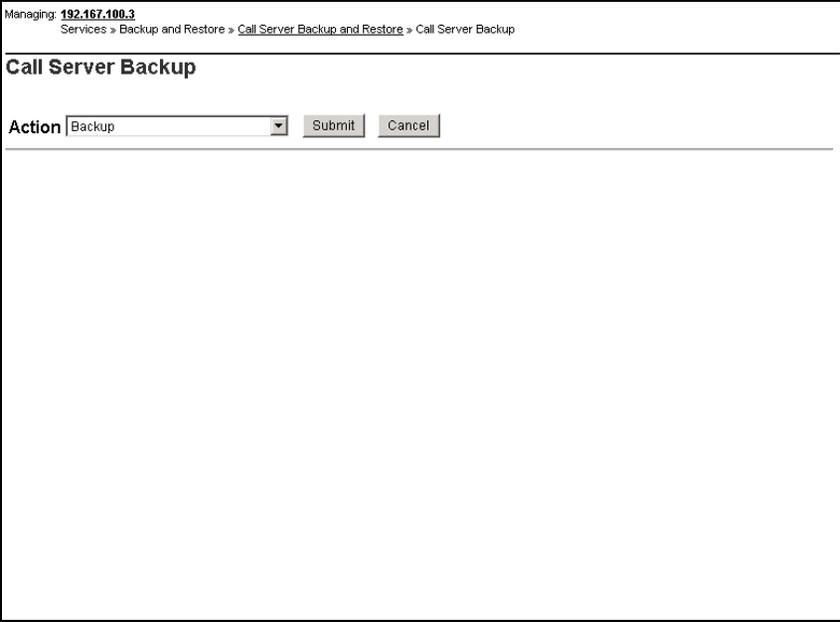


*Note:* Backup Rules and Backup Schedules are available only on CPP II and CPP IV systems.

### Backup

To back up the Call Server, click the **Backup** link on the **Call Server Backup and Restore** web page. The **Call Server Backup** web page opens, as shown in [Figure 110 on page 215](#).

**Figure 110**  
**Call Server Backup web page**



Managing: 192.167.100.3  
Services > Backup and Restore > Call Server Backup and Restore > Call Server Backup

### Call Server Backup

Action

Select **Backup** from the **Action** drop-down list and click **Submit**. The **Call Server Backup Waiting** web page opens to indicate that the backup is in progress.

The Backup function invokes a data dump and writes the Call Server data to the primary and internal backup drives.

The Backup function performs the same task as the EDD CLI command traditionally configured in LD 43.

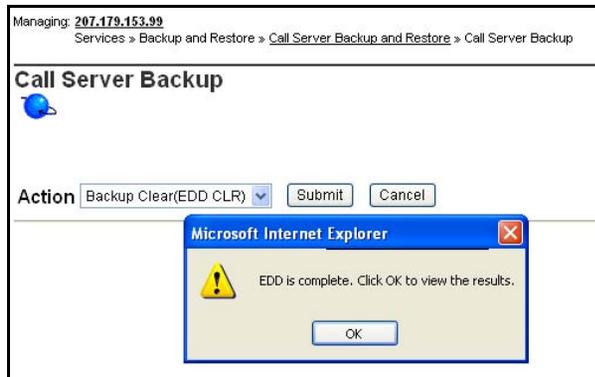
When the backup has finished, a dialog box appears to indicate that the Equipment Data Dump (EDD) is complete. Click **OK**.

A summary of the results of the EDD appears at the bottom of the **Call Server Backup** web page.

## Performing manual database replication

To manually invoke the database replication process on a Small System, on the **Call Server Backup** web page select **Backup Clear** from the **Action** drop-down list, and click **Submit**. When the restore is complete, a message box appears. See [Figure 111](#).

**Figure 111**  
**EDD Complete**



Click **OK** to view the results.

To manually invoke the database replication process on a Large System, select **Backup According to Rule** from the **Action** drop-down list, and click **Submit**. The **Backup Rule Number** drop-down list appears. In the **Backup Rule Number** drop-down list, enter the Backup Rule number to use for the restore operation. Click **Submit**. When the restore is complete, a message box appears. See [Figure 111](#).

Click **OK** to view the results.

For more information on backing up and restoring databases for Geographic Redundancy, see *Communication Server 1000: System Redundancy* (553-3001-307).

## Restore

The Call Server Restore function restores the backed-up files from the internal backup device to the primary device. The Restore function performs the same task as the CLI RIB command traditionally configured in LD 43.



### **WARNING**

The process to restore data using the Element Manager interface is immediate. There is no warning or detailed information provided on the specifics of the data to be restored.

Also, note that a “cold start” of the system is required before the restored data is in effect.

Click the **Restore** link on the **Call Server Backup and Restore** web page. The **Call Server Restore** web page opens (see [Figure 112 on page 218](#)).

**Figure 112**  
**Call Server Restore web page**

Managing: 192.167.100.3  
Services > Backup and Restore > Call Server Backup and Restore > Call Server Restore

### Call Server Restore

Action | Restore from Backup Data(RES) | Submit | Cancel

Select **Restore from Backup Data (RES)** in the **Action** drop-down list, and click **Submit**.

*Note:* The database for Element Manager IP Telephony is updated immediately after the restore. Other call server databases require a cold start after the restore.

For information about the server databases and when they were created, select **Database issue and creation date** in the **Action** drop-down list, and click **Submit**. The information is displayed in the text area below the command.

To manually invoke a database restore process, select **Restore According to Rule (RSR X Y)** from the **Action** drop-down list. The **Backup Rule Number** and **Restore Version** drop-down lists appear.

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

For more information on backing up and restoring databases for Geographic Redundancy, see *Communication Server 1000: System Redundancy* (553-3001-307).

## Backup Rules

To add or edit a Backup Rule, click the **Backup Rules** link on the **Call Server Backup and Restore** web page. The **Backup Rules** web page opens as shown in [Figure 113](#).

**Figure 113**  
**Backup Rules web page**

Managing: 192.167.100.3  
Services > Backup and Restore > Call Server Backup and Restore > Backup Rules

### Backup Rules

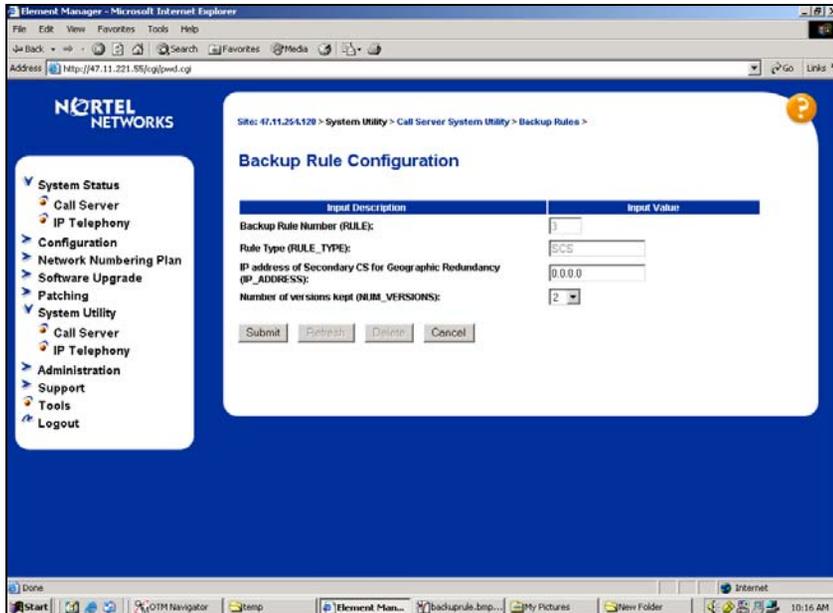
Choose a Backup Rule: 2

Rule	Type	Name	IP address	User Name	Versions kept	Edit	Delete	Backup History
1	SCS	BACKUP1	0.0.0.0		2	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Backup History"/>

To view a log of backup attempts, click the **Backup History** button. The **Backup History** web page opens. This web page displays information for each backup attempt based on the given Backup Rule.

To add a Backup Rule, click the **to Add** button on the **Backup Rules** web page. To edit a Backup Rule, click the **Edit** button. In both cases, the **Backup Rule Configuration** web page opens, as shown in [Figure 114 on page 220](#).

**Figure 114**  
**Backup Rule Configuration**



The following Backup Rule Types are available:

- Fixed Media Device (FMD).
- FTP (FTP)
- Secondary Call Server (SCS)
- Removable Media Device (RMD)

For more information on configuring backup rules for Geographic Redundancy, see *Communication Server 1000: System Redundancy* (553-3001-307).

### Backup Schedules

Backup schedules provide the user with the ability to schedule backup operations associated with a specified backup rule. To add or edit a Backup Schedule, click the **Backup Schedules** link on the **Call Server Backup and**

**Restore** web page. The **Backup Schedules** web page opens as shown in [Figure 115](#)

**Figure 115**  
**Backup Schedules web page**

Managing: [192.167.100.3](#)  
Services > Backup and Restore > [Call Server Backup and Restore](#) > Backup Schedules

### Backup Schedules

Choose a Backup Schedule:

Schedule Number	Rule Number	Rule Name	Rule Type	Frequency	Day	Hour	Edit	Delete
1	1	BACKUP1	SCS	Monthly	1	1	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

To add a Backup Schedule, click the **to Add** button. To edit a Backup Schedule, click the **Edit** button. In both cases, the **Backup Schedule Configuration** web page opens, as shown in [Figure 116](#) on [page 222](#).

**Figure 116**  
**Backup Schedule Configuration**

Managing: [192.167.100.3](#)  
Services > Backup and Restore > [Call Server Backup and Restore](#) > [Backup Schedules](#) > Backup Schedule Configuration

### Backup Schedule Configuration

Input Description	Input Value
Backup Schedule Number:	<input type="text" value="2"/>
Backup Rule:	<input type="text" value="1"/>
Backup Rule Name:	<input type="text" value="BACKUP1"/>
Backup Rule Type:	<input type="text" value="SCS"/>
Frequency:	<input type="text" value="Monthly (M)"/>
Day:	<input type="text" value="1"/>
Hour:	<input type="text" value="0"/>

Each backup schedule defines a total of five associated parameters, as follows:

- **Backup Schedule Number** — up to ten backup schedules can be defined, numbered from one to ten.
- **Backup Rule** — specifies the backup rule number associated with this backup schedule. The backup rule number must be previously configured.
- **Frequency** — defines how often the scheduled backup operation occurs. The default is D. Not more than one backup schedule can be defined with Frequency set to the value A. Options are:
  - M (monthly)
  - W (weekly)

- D (daily)
- A (automatic — immediately after every EDD)
- **Day** — specifies the day on which the backup occurs with a default value of SU. When Frequency is M, the range is 1 to 31 with a default value of 1. This parameter does not apply when Frequency is set to either of the values D or A. When Frequency is W, the range is the days of the week as follows:
  - SU
  - MO
  - TU
  - WE
  - TH
  - FR
  - SA
- **Hour** — specifies the hour in the day on which the backup occurs. The range is 0 to 23, with a default of 3. This parameter does not apply when FREQ is set to the value A.

Backup schedules are supported only on CP PII and CP PIV systems. A backup schedule can be created, modified, deleted, and printed by the respective command options NEW, CHG, OUT, and PRT.

## Personal Directories Backup and Restore

For information on Backup and Restore functions of Personal Directories, See “Personal Directories” on [page 161](#).

## Date and Time

The Date and Time function enables users to use Element Manager to modify the system’s current time and date. The Date and Time function performs the same task as the CLI STAD command traditionally configured in LD 02.

**Note 1:** The date and time configured in either Element Manager or LD 02 is synchronized to all primary Signaling Servers and IP Telephony Leaders within the system. Users can specify, on a node basis, whether the Simple Network Transfer Protocol (SNTP) server (running on the primary Signaling Server) or the IP Telephony Leader cards actively push the date and time to the SNTP clients (IP Line 4.0/Voice Gateway cards and other Signaling Servers) or if the SNTP clients pull the date and time from the SNTP server.

**Note 2:** Synchronization can be set to occur on a regular interval, when modifications are made, or during a data dump, including a midnight routine data dump. As part of the Node configuration, users can specify how the date and time are propagated within the Node by configuring the primary Signal Servers or IP Telephony Leaders to run in broadcast mode or listen mode.

Click the **Date and Time** link in the **Services** branch of the Element Manager navigator. The **System Date and Time** web page opens, as shown in [Figure 117 on page 225](#).

**Figure 117**  
**System Date and Time web page**

Managing: **192.167.100.3**  
 Services > System Date and Time

---

**System Date and Time**

Input Description	Input Value
Year (YEAR):	<input type="text" value="2005"/>
Month (MON):	<input type="text" value="06"/>
Day (DAY):	<input type="text" value="13"/>
Hour (HOUR):	<input type="text" value="13"/>
Minute (MIN):	<input type="text" value="42"/>
Second (SEC):	<input type="text" value="53"/>
Day Of Week (WEEK):	<input type="text" value="MON"/>

\*Note: In Week field change will be noticed only on refresh or submit

To modify the date and time, enter the current date and time in the **Input Value** text boxes, and click **Submit**.

*Note:* The valid range for Month (MON) is 1 through 12. Entering a value higher than 12 disables the **Refresh** button.

## Logs and Reports

For information on IP Telephony Node Maintenance and Reports, see “Nodes: Servers, Media Cards” on [page 128](#).

In addition, information about the database status and synchronization are available under the Reports tab in NRS Manager. For more information on these reports, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

To view a list of software feature packages, click the **Logs and Reports > Equipped Feature Packages** link in the **Services** branch of the Element Manager navigator. The **Equipped Feature Packages List** web page opens as shown in [Figure 118](#).

**Figure 118**  
**Equipped Feature Packages List web page**

Managing: 192.167.100.3  
Services > Logs and Reports > Equipped Feature Packages List

### Equipped Feature Packages List

Package Description	Package Number
Optional Features (OPTF)	1
Multi-Customer Operation (CUST)	2
Call Detail Recording, Teletype Terminal (CDR)	4
Call Detail Recording, Teletype Terminal (CTY)	5
Recorded Announcement (RAN)	7
Time and Date (TAD)	8
Do Not Disturb Individual (DNDI)	9
End-to-End Signaling (EES)	10
Intercept Treatment (INTR)	11
Automatic Number Identification (ANI)	12
Automatic Number Identification, Route Selection (ANIR)	13
Basic Routing (BRTE)	14
1.5-Mbit Remote Peripheral Equipment (RPE1.5)	15
Do Not Disturb Group (DNDG)	16
Make Set Busy (MSB)	17
Special Service for 2500 Sets (SS25)	18
Digit Display (DDSP)	19
Office Data Administration System (ODAS)	20
Dial Intercom (DI)	21
Direct Inward System Access (DISA)	22
Charge Account for CDR (CHG)	23
Charge Account/Authorization code (CAB)	24
Basic Authorization code (BAUT)	25
Centralized Attendant Service (Main) (CASM)	26
Centralized Attendant Service (Remote) (CASR)	27

To view a list of Call Server reports available on a Small System, click the **Logs and Reports > Call Server Report Utility** link in the **Services** branch of the Element Manager navigator. The **Call Server Report Utility** web page opens as shown in [Figure 119](#) on [page 227](#).

**Figure 119**  
**Call Server Report Utility web page - Small System**

Managing: 47.11.193.130  
 Services > Logs and Reports > PDT Password Portal > Call Server Report Utility

### Call Server Report Utility

		<input type="button" value="RDOPEN"/>	<input type="button" value="RDSHOW"/>	<input type="button" value="SYMLOAD"/>
Display Latest Records	<input type="text" value="16"/>	<input type="button" value="RDTAIL"/>		
Display Oldest Records	<input type="text" value="16"/>	<input type="button" value="RDHEAD"/>		
Display Record Number	<input type="text" value="668"/>	<input type="button" value="RDGO"/>		
Skip Records	<input type="text" value="0"/>	Display Records	<input type="text" value="1"/>	<input type="button" value="RD"/>
Skip Records	<input type="text" value="0"/>	Display Records	<input type="text" value="1"/>	<input type="button" value="RDS"/>
Start Record Number	<input type="text" value="0"/>	Display Records	<input type="text" value="1"/>	<input type="button" value="VIEW"/>
Backup Time (Hours)	<input type="text" value="20"/>	<input type="button" value="RDBACKUP"/>	<input type="button" value="RDBACKUPSHOW"/>	

Click a button to invoke a command.

To view a list of Call Server reports available on a Large System, click the **Logs and Reports > Call Server Report Utility** link in the **Services** branch of the Element Manager navigator. The **Call Server Report Utility** web page opens as shown in Figure 120 on [page 228](#).

**Figure 120**  
**Call Server Report Utility web page - Large System**

The buttons at the top of these web pages provide access to the following functions:

- **RDOPEN** - Opens the latest report file
- **RDSHOW** - Shows a summary of the report file
- **RDTAIL** - Shows *x* records up to the newest record in the report file (where *x* is the configured display size).
- **RDHEAD** - Shows *x* records starting from the oldest record in the report file (where *x* is the configured display size).

To view selected detail data on records in the report file, use the text boxes, drop-down lists, and the following buttons:

- **RDGO** - Displays the record specified in the adjacent text box (where -1 is the oldest record, 1000 is the most recent).

- **RD** - Browses the report records. Enter the number of records to skip and the number of records to display in the adjacent text boxes.
- **RDS** - Browses the report records with (symbolic) memory dump. Enter the number of records to skip, and select the number of records to display using the adjacent text box and drop-down list.
- **VIEW** - Views selected records. Enter a starting record number and select the number of records to view using the adjacent text box and drop-down list. Negative numbers indicate records previous to the starting record.

The results are displayed in the text box at the bottom of the web page.

To view a list of Peripheral Software Version Data, click the **Logs and Reports > Peripheral Software Version Data** link in the **Services** branch of the Element Manager navigator. The **Peripheral Software Version Data** web page opens as shown in [Figure 121](#).

**Figure 121**  
**Peripheral Software Version Data web page**

Managing: 192.167.100.3  
Services > Logs and Reports > Peripheral Software Version Data

### Peripheral Software Version Data

PSWV Version: 115    MDCS Version:

Peripheral Software Application	Version Number
Extended Network Card (XNET)	23
Carrier Remote IPE Card (LCRI)	02
Extended Peripheral Equipment Controller Card (XPEC)	40
Multipurpose ISDN Signalling Link Basecode Loadware (MISP)	71
MISP BRI Line Application Loadware (BRIL)	83
MISP BRI Trunk Application Loadware (BRIT)	82
MISP Meridian Packet Handler Application Loadware (MPH)	51
Multipurpose Serial Data Link Basecode Loadware (MSDL)	73
MSDL ASYN Application (SDI)	51
MSDL DCH Application (DCH)	72
MSDL Application Module Link Application (AML)	81
BRSC Basecode (BRSC)	71
BRSC BRI Application (BBRI)	54
UIPE PRI Loadware Application (PRIE)	84
UIPE BRIT Loadware Application (BRIE)	86
N12 TR1268 Datafile (NI02)	26
ISO QSIG PRI2 Interface Datafile (ISIG)	33
NEW ZEALAND Interface Datafile (TCNZ)	13
ETSI Interface Datafile (ETSI)	48
AUSTRIA Interface Datafile (AUS1)	48
DENMARK Interface Datafile (DEN1)	48
FINLAND Interface Datafile (FIN1)	48
GERMANY Interface Datafile (GER1)	53

To view a list of System Licence Parameters, click the **Logs and Reports > System Licence Parameters** link in the **Services** branch of the Element Manager navigator. The **System Licence Parameters** web page opens as shown in [Figure 122](#).

**Figure 122**  
**System Licence Parameters web page**

Managing: [192.167.100.3](#)  
Services > Logs and Reports > System Licence Parameters

### System Licence Parameters

NAME	LIMIT	LEFT	USED
ANALOGUE TELEPHONES	32767	32767	0
CLASS TELEPHONES	32767	32767	0
DIGITAL TELEPHONES	32767	32767	0
DECT USERS	32767	32767	0
IP USERS	32767	32759	8
BASIC IP USERS	32767	32767	0
DECT VISITOR USER	32767	32767	0
ACD AGENTS	32767	32767	0
PCA	32767	32767	0
ITG ISDN TRUNKS	32767	32767	0
H.323 ACCESS PORTS	32767	32767	0
AST	32767	32767	0
RAN CON	32767	32767	0
MUS CON	32767	32767	0
TNS	32767	32721	46
ACDN	24000	23994	6
AML	32	30	2
IDLE_SET_DISPLAY	NORTEL		
LTID	100	100	0
RAN RTE	32767	32767	0
ATTENDANT CONSOLES	32767	32767	0
BRI DSL	100	100	0
MPH DSL	100	100	0
DATA PORTS	32767	32767	0
PHANTOM PORTS	32767	32760	7

---

# Security

---

## Contents

This section contains information on the following topics:

<a href="#">Introduction</a> . . . . .	231
<a href="#">System Passwords</a> . . . . .	231
<a href="#">SSL/TLS</a> . . . . .	235
<a href="#">Security Alerts</a> . . . . .	235

## Introduction

Security applies to Element Manager in the following forms:

- System Passwords
- SSL/TLS

## System Passwords

The password information that is available to the user depends on the login ID used to log in to Element Manager.

Users who log in with an Administrator level password can create login names and passwords for other users to limit access to certain aspects of Element Manager functionality.

Users who log in with a login name and password assigned by the administrator can access only functionality configured for their login name. There are two password account levels:

- Level2 Password (PWD2) account: This user can access all components available from the Call Server user interface.
- Level1 Password (PWD1) account: This user can access all maintenance and administration overlays.

For more information on system password account levels, see *System Security Management (553-3001-302)*.

When a user clicks the **Security > System Passwords** link in the **Services** branch of the Element Manager navigator, the **Password Accounts List** web page opens (see [Figure 123](#)). The information that the administrator has configured for the user's password appears on this page.

**Figure 123**  
**Password Account web page**

The screenshot shows a web interface for managing password accounts. At the top, it indicates the user is managing IP 207.179.153.99 and is in the 'Services > Security > Password Accounts List' section. The main heading is 'Password Accounts List'. Below this, a specific account is highlighted: '- Limited Access Password -- DAVID', with an 'Edit' button to its right. The account details are as follows:

- User Name: DAVID
- Allowed: 001 002 010 011 012 013 014 015 016 017 018 019 020 021 022 023 024 025 026 027 028 029 030 031 032 033 034 036 037 038 039 040 043 044 045 046 048 049 050 051 052 053 054 056
- Overlay List: 057 058 060 061 062 066 073 074 075 077 079 080 081 082 083 084 086 087 088 090 092 093 094 095 096 097 117 135 137 143
- Accessible Customer: ALL
- Enable Host Mode Log In: NO
- Enable MAT Log In: YES
- Options: PSCA RDBA CFPA LLCA PROA LOSA FORCA MONA

## PDT Passwords

There are two PDT Password account levels:

- PDT Level2 Password (PDT2) account: This user can access the PDT prompt of the Call Server to perform various corrective actions, such as patching.
- PDT Level1 Password (PDT1) account: This user can acquire various types of information required for recovering faulty systems.

Users with PDT Level2 access can change the PDT passwords. To open the **PDT Password Change** web page (see [Figure 124](#)), click the **Security > PDT Passwords** link in the **Services** branch of the Element Manager navigator.

**Figure 124**  
**PDT Password Change web page**

Managing: [192.167.100.3](#)  
Services > Security > PDT Password Change

---

### PDT Password Change

Input Description	Input Value
Old PDT Level2 Password	<input type="text"/>
New PDT Level2 Password(PDT2)	<input type="text"/>
Re-enter Password(PDT2)	<input type="text"/>
New PDT Level1 Password(PDT1)	<input type="text"/>
Re-enter Password(PDT1)	<input type="text"/>

Note: Changing PDT passwords will trigger an automatic EDD for password synchronization.

To change PDT passwords, enter the Old PDT Level2 Password, followed by the new PDT Level2 and PDT Level1 passwords.

## Shell Login Options

To open the **Shell Login Options** web page (see [Figure 125 on page 234](#)), click the **Security > Shell Login Options** link in the **Services** branch of the Element Manager navigator.

**Figure 125**  
**Shell Login Options web page**

Managing: 192.167.100.3  
Shell Login Options

### Shell Login Options

Diagnostic Commands	Action
DIS SHELLS INSECURE - Disable the insecure shells in the systems(Telnet,rlogin,FTP)	Submit

Instruction: Select command, and click on [Submit]

Cancel View page log

Use this web page to run Shell Login Options commands. Select a command from the drop-down list and click **Submit**. The results are displayed in the text area.

## SSL/TLS

When the user clicks the **Security > SSL/TLS** link in the **Services** branch of the Element Manager navigator, the **SSL/TLS Service Configuration** web page opens, as shown in [Figure 126 on page 235](#).

**Figure 126**  
**SSL/TLS Service Configuration web page**

Managing **Buffv 1 (47.11.139.4)**  
SSL/TLS Service Configuration

---

### SSL/TLS Service Configuration

SSL/TLS Service Status	
<b>Service Status</b>	There is no certificate installed on your service and also there is no pending request for certificate.
Current Certificate Details	
<b>Friendly Name</b>	not available
<b>Expiration Date</b>	not available
<b>Issued To</b>	not available
<b>Issued By</b>	not available
Service Options	
<b>Usage Rule</b>	not available <input type="button" value="Edit..."/>
<b>SSL/TLS Port</b>	not available <input type="button" value="Edit..."/>

See “Certificate Management” on [page 239](#) for more information on creating and managing security certificates.

## Security Alerts

When using the SSL Service to access Element Manager and NRS Manager, there are instances when Security Alerts may appear:

- when establishing the initial connection to Element Manager or NRS Manager over a secure port (for example https)
- when launching a Virtual Terminal Emulator session from within a secure Element Manager session

While establishing the initial connection to Element Manager or NRS Manager, the following Security Alerts may appear. These alerts are generated by Internet Explorer:

- 1 "The security certificate has been generated by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority."

This alert will be presented when a self signed certificate is being used. In order to avoid seeing this alert in the future, the certificate can be installed into the browser's trusted list.

- 2 "The name on the security certificate is invalid, or does not match the name of the site."

This alert will be presented when the common name within the certificate does not match the hostname being used to access Element Manager or NRS Manager. It will also be generated if DNS is not being used and Element Manager or NRS Manager is being accessed through its IP address.

While launching a Virtual Terminal session from within a secure Element Manager session, the following Security Alerts may appear. These alerts are generated by the Java Runtime Environment (JRE):

- 1 "The security certificate was issued by a company that is not trusted."

This alert will be presented when a self signed certificate is being used. In order to avoid seeing this alert in the future, the certificate can be installed into the browser's trusted list.

- 2 "The hostname in the server security certificate does not match the name of the server."

This alert will be presented when the common name within the certificate does not match the hostname being used to access Element Manager or NRS

Manager. It will also be generated if DNS is not being used and Element Manager or NRS Manager is being accessed via its IP address.



---

# Certificate Management

---

## Contents

Overview . . . . .	240
Creating a new certificate request . . . . .	240
Processing a pending certificate response . . . . .	241
Deleting a pending certificate request . . . . .	242
Creating a self-signed certificate . . . . .	242
Assigning an existing certificate . . . . .	243
Importing a certificate and its private key . . . . .	244
Creating a certificate renew request for the current certificate . . . . .	244
Removing the current certificate . . . . .	245
Replacing the current certificate . . . . .	246
Exporting the current self-signed certificate . . . . .	246
Exporting the current certificate and its private key . . . . .	247
SSL/TSL security configuration . . . . .	248

## Overview

This section contains information on the Element Manager SSL/TLS Service Management Wizard, which guides users through the certificate management and Transportation Layer Security (TLS) configuration process.

## Creating a new certificate request

When Element Manager is first deployed, no certificate is installed. The TLS service for the Element Manager is disabled.

Follow the steps in Procedure 7 to create a new certificate request.

### **Procedure 7** **Creating a new certificate request**

- 1 Log in using the non-secure mode.
- 2 Click **Configure**.  
The **Server Certificate** web page appears.
- 3 Select the **Create a new certificate request to be signed by Certificate Authority** radio button and click **Next**.  
The **Name and Security Settings** web page appears.
- 4 Enter a **Friendly Name** for the certificate.
- 5 Select a bit length from the **Bit length** drop-down list.
- 6 Click **Next**.  
The **Organization Information** web page appears.
- 7 Enter an **Organization** and **Organization Unit** and click **Next**.  
The **Your Server's Common Name** web page appears.
- 8 Enter a **Common Name** and click **Next**.  
The **Geographical Information** web page appears.
- 9 Enter a **Country/Region**.
- 10 Enter a **State/Province**.
- 11 Enter a **City/Locality**.
- 12 Click **Next**.

The **Certificate Request Summary** web page appears.

- 13 Click **Commit** to download the certificate request to a local file.

The **X.509 Certificate Request** web page appears.

- 14 Click **Close** to close the wizard.

---

**End of Procedure**

---

## Processing a pending certificate response

The certificate request file is submitted to a Certificate Authority. The Certificate Authority sends a response in a text file.

Follow the steps in Procedure 8 to process the pending certificate response file.

### **Procedure 8**

#### **Processing a pending certificate response**

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.

The **Server Certificate** web page appears.

- 2 Select the **Process the pending request and install the certificate** option button and click **Next**.

The **Process a Pending Request** web page appears.

- 3 Copy the contents of the text file received from the certificate authority.

- 4 Click **Commit**.

The **Certificate Summary** web page appears.

- 5 Click **Finish**.

---

**End of Procedure**

---

To verify that the Certificate Authority is trusted by Internet Explorer, choose **Tools > Internet Options > Content > Certificates**. The **Trusted Certificate Authority List** web page appears.

If the Certificate Authority is not in the trusted Certificate Authority list of Internet Explorer, a **Security Alert** web page appears when accessing Element Manager using SSL or TLS.

The user must then log in using the secure mode.

## Deleting a pending certificate request

Follow the steps in Procedure 9 to delete a pending certificate request.

### Procedure 9 Deleting a pending certificate request

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.  
The **Server Certificate** web page appears.
- 2 Select the **Delete the pending request** option button and click **Next**.  
The **Delete a Pending Request** web page appears.
- 3 Click **Finish**.

————— End of Procedure —————

## Creating a self-signed certificate

Follow the steps in Procedure 10 to create a self-signed certificate.

### Procedure 10 Creating a self-signed certificate

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.  
The **Server Certificate** web page appears.
- 2 Select the **Create a new self-signed certificate** option button and click **Next**.  
The **New Self-Signed Certificate** web page appears.
- 3 Click **Next**.  
The **Name and Security Settings** web page appears.
- 4 Enter a **Friendly Name** for the certificate.

- 5 Select a bit length from the **Bit length** drop-down list.
- 6 Click **Next**.  
The **Organization Information** web page appears.
- 7 Enter an **Organization** and **Organization Unit** and click **Next**.  
The **Your Server's Common Name** web page appears.
- 8 Enter a **Common Name** and click **Next**.  
The **Geographical Information** web page appears.
- 9 Enter a **Country/Region**.
- 10 Enter a **State/Province**.
- 11 Enter a **City/Locality**.
- 12 Click **Next**.  
The **Certificate Request Summary** web page appears.
- 13 Click **Commit**.  
The **X.509 Certificate Request** web page appears.
- 14 Click **Close** to close the wizard.  
If the **Security Alert** web page appears, click **Yes**.

*Note:* The user can also export the self-signed certificate and distribute it into the trusted Certificate Authority list of Internet Explorer.

---

**End of Procedure**

---

## Assigning an existing certificate

To assign an existing certificate to the Element Manager's web site, follow the steps in Procedure 11 on [page 243](#).

### **Procedure 11** **Assigning an existing certificate**

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.  
The **Server Certificate** web page appears.
- 2 Select the **Assign an existing certificate** option button and click **Next**.

The **Available Certificate** web page appears.

- 3 Select a certificate from the list of available certificates and click **Next**.

The **Certificate Summary** web page appears.

- 4 Click **Finish**.

---

**End of Procedure**

---

## Importing a certificate and its private key

Follow the steps in Procedure 12 to import a certificate and its private key.

### Procedure 12

#### Importing a certificate and its private key

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.

The **Server Certificate** web page appears.

- 2 Select the **Import a certificate and its private key from a PEM encoded file** option button and click **Next**.

The **Import Certificate Password** web page appears.

- 3 Enter the password of the certificate file and click **Commit**.

The **Import Certificate** web page appears.

- 4 Copy the contents of the text file received from the certificate authority.

- 5 Click **Commit**.

The **Certificate Summary** web page appears.

- 6 Click **Finish**.

---

**End of Procedure**

---

## Creating a certificate renew request for the current certificate

The X.509 certificate has an expiration date. A warning message is shown if the expiration date is less than one month away. To create a certificate renewal request, follow the steps in Procedure 13.

**Procedure 13****Creating a certificate renew request**

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.  
The **Server Certificate** web page appears.
- 2 Select the **Create a certificate renew request** option button and click **Next**.  
The **Certificate Request Summary** web page appears.
- 3 Click **Commit** to download the certificate request to a local file.  
The **X.509 Certificate Request** web page appears.
- 4 Click **Close** to close the wizard.

---

**End of Procedure**

---

## Removing the current certificate

To remove a current certificate, follow the steps in Procedure 14.

**Procedure 14****Removing the current certificate**

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.  
The **Server Certificate** web page appears.
- 2 Select the **Remove the current certificate** option button and click **Next**.  
The **Remove a Certificate** web page appears.
- 3 Click **Finish**.

*Note:* All client sessions must be terminated before the removing operation can take effect.

---

**End of Procedure**

---

## Replacing the current certificate

To replace the current certificate, follow the steps in Procedure 15.

*Note:* The security context of the Web SSL service will change to the new certificate when there is no active HTTPS connection.

### Procedure 15 Replacing the current certificate

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.  
The **Server Certificate Configuration Wizard** web page appears.
- 2 Select the **Replace the current certificate** option button and click **Next**.  
The **Available Certificate** web page appears.
- 3 Select a certificate from the list and click **Next**.  
The **Certificate Summary** web page appears.
- 4 Click **Close** to close the wizard.

---

End of Procedure

---

## Exporting the current self-signed certificate

When the current certificate is self-signed, it can be exported. Using SSL and TLS protocol, the certificate file can be used to set up a trust relationship between different parties.

To export the current self-signed certificate, follow the steps in Procedure 16.

### Procedure 16 Exporting the current self-signed certificate

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.  
The **Server Certificate Configuration Wizard** web page appears.
- 2 Select the **Export the current self-signed certificate** option button and click **Next**.  
The **Export Self-signed Certificate Summary** web page appears.
- 3 Click **Download**.

The **Certificate Content** web page appears. Copy the contents of the text box and save it as a plain text file. When exporting the self-signed certificate, name the file with extension .cer. The file can then be installed in the trusted certificate list of the client.

- 4 Click **Close** to close the wizard.

---

**End of Procedure**

---

## Exporting the current certificate and its private key

The current certificate and its private key can be exported. A password is required to encrypt the file. Use the same password that was used to import the file.

Follow the steps in Procedure 17 to export the current certificate and its private key.

### **Procedure 17**

#### **Exporting the current certificate**

- 1 On the **SSL/TLS Service Configuration** web page, click **Configure**.

The **Server Certificate Configuration Wizard** web page appears.

- 2 Select the **Export the current certificate and its private key** option button and click **Next**.

The **Export Certificate Password** web page appears.

- 3 Enter the password and click **Next**.

The **Export Current Certificate and Private Key Summary** web page appears.

- 4 Click **Download**.

The **Certificate Content** web page appears. When exporting the certificate and private key, import the file to another server.

- 5 Click **Close** to close the wizard.

---

**End of Procedure**

---

## SSL/TSL security configuration

When a certificate is installed on Element Manager, the SSL/TLS usage rule is set to “Always” by default.

If "Always" is selected, all user traffic must use SSL/TLS. If "UserChoice" is selected, users can choose between secure and non-secure sessions when they log in.

The user can configure the TCP port used by the SSL and TLS service by entering a value in the **SSL/TLS** field. The default value is 443.

# Support

---

## Contents

This section contains information on the following topics:

<a href="#">Introduction</a> . . . . .	249
<a href="#">Help</a> . . . . .	250
<a href="#">Release Notes</a> . . . . .	250

## Introduction

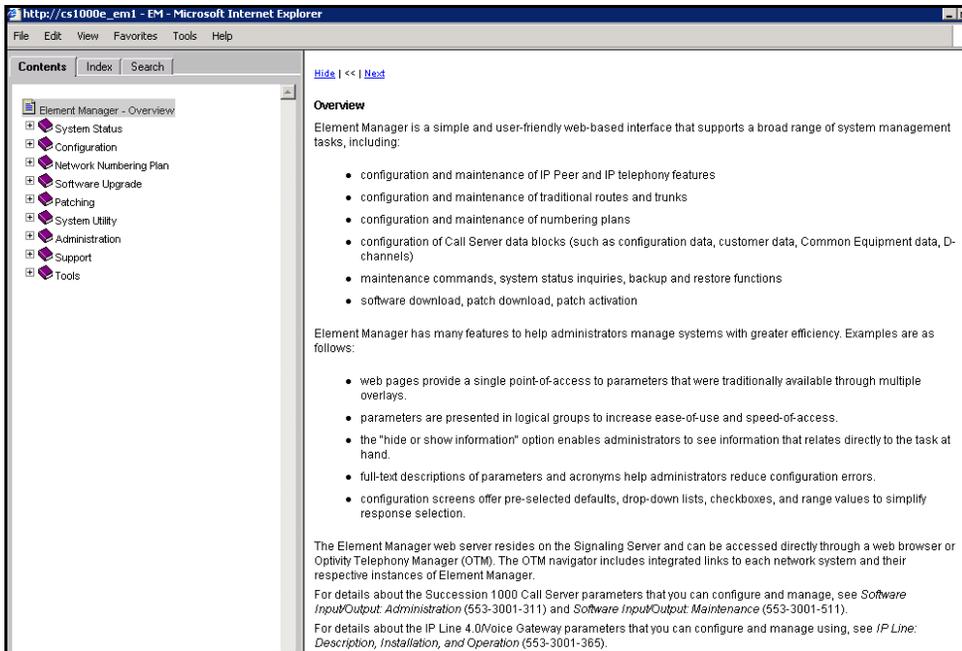
The following Support features can be accessed through Element Manager:

- [Help](#)
- [Release Notes](#)

## Help

Element Manager provides context-sensitive online Help. To access Help, click the **Help** link located in the top right corner of the Element Manager web pages. The **Help** web page shown in [Figure 127](#) opens.

**Figure 127**  
**Help web page**



## Release Notes

A Release Note can describe a design change or a product feature that was discovered after market release. Often, a Release Note describes how to work around a product limitation. Click the **Release Notes** link to access the web-based Helmsman Express application.

---

# Index

---

## A

ABCD Bit Signaling Category, 193  
ABKUP, 117  
access levels, 204  
ACOD, 180  
ADAN, 191  
add a Virtual Terminal Session, 33  
add Bookmark, 36  
administrator, 231  
Advanced Configurations, 184  
Advanced Trunk Configuration, 187  
ADVOPT, 191  
AML, 45  
AML Diagnostics, 45  
ANAT, 171  
ANI. *See* Automatic Number Identification.  
ANLD, 171  
ARSTR, 117  
ASYSLD, 117  
ATLP, 71  
ATST, 94  
Automatic Number Identification, 171

## B

Background Signaling and Switching diagnostics,  
47

Backup, 213  
Basic Rate Line Interface, 193  
Basic Rate Trunk Interface, 193  
Basic Route Options, 181  
BILN, 181  
BKUP\_RULE, 117  
Bookmarks  
    delete, 37  
    edit, 37  
Bookmarks, add, 36  
Boss Secretary Filtering Enhancement, 172  
Branch Office  
    Basic Property and Bandwidth Management,  
    148  
Branch Office (553-3001-214), 148  
BRIL. *See* Basic Rate Line Interface.  
BRIT. *See* Basic Rate Trunk Interface.  
BRSC, 98  
BSCOPT, 191  
BSFE, 172

## C

Calling Line Identification, 173  
Call Server, 14, 29, 40, 111, 197, 206  
    backup, 215  
    restore, 217  
Call Server Select by Functionality, 40

Call Server Select by Overlay, 42  
Call Server Virtual Terminal Session, 33  
Call Trace Diagnostics, 49  
cancel, 29, 40  
CDP. *See* Coordinated Dialing Plan.  
CDR, 181  
CDSP, 60, 75, 84, 94, 102, 106, 109  
CEQU. *See* common equipment.  
CHG ZQNL, 81  
CLID. *See* Calling Line Identification.  
clock controller, 54, 194  
Clock Controller Diagnostic, 53  
CLR GR, 61  
CLS, 186  
CMAJ, 60, 94, 102, 107  
CMIN, 60, 75, 84, 94, 102, 109  
CMIN ALL, 60, 75, 84, 94, 102, 106, 109  
CNTL, 181  
CNVT, 181  
Code Restriction Tree Number, 207  
Collaborative Server, 201  
common equipment, 111  
community strings, 115  
CONF\_DSP, 172  
Conference Display, 172  
Conference loop numbers, 112  
configuration, 29, 40, 180  
Configuration menu, 13, 26  
Configuration Record, 191  
Coordinated Dialing Plan, 198, 199  
Core Common Equipment Diagnostics, 55  
    Large System, 57  
    Small System, 56  
CPED, 102  
CRNO. *See* Code Restriction Tree Number.

customer, 170, 206, 209  
Customer Data Block, 170, 171, 172, 173  
Customer Explorer, 169  
CUTOVR, 60

## D

Database issue and creation date, 218  
Database Replication Control, 116  
D-channel, 64  
D-channel Diagnostics, 64  
D-Channel Expansion Diagnostics, 66  
D-channel Property Configuration, 191  
DDB. *See* Digital Trunk Interface Data Block.  
delete, 29  
delete Bookmarks, 37  
DES, 180, 185  
DGT. *See* Digit Manipulation Block.  
Diagnostic Commands, 100  
Digital Trunk Card, 69  
Digital Trunk Card Diagnostic, 68  
Digital Trunk Interface, 193, 196  
Digital Trunk Interface and Primary Rate Interface  
    Clock Controller Diagnostics, 53  
Digital Trunk Interface and Primary Rate Interface  
    Diagnostic, 54, 69  
Digital Trunk Interface Data Block, 192, 193, 196  
Digital Trunk Interface Loop numbers, 112  
Digital Trunk Maintenance Diagnostics, 73  
Digital Trunk Route, 71  
Digit Conversion Tree Number, 210  
Digit Manipulation Block, 199  
digit sequences, 208  
DIS, 89, 104  
DIS AML, 46  
DIS AUTO, 65, 99

DISC, 93, 97, 98, 99, 108  
DISC BRI, 98  
DISC BRIE, 98  
DIS CC, 54, 55  
DIS CNI, 59  
DIS DCH, 65  
DIS DDSC, 74  
DIS DDSL, 74  
DIS DTCS, 74  
DIS DTRC, 74  
DIS DTSL, 74  
DIS DTVC, 74  
DIS ELAN, 46  
DIS FIL, 57  
DISI, 69  
DISI DDSC, 74  
DISI DTCS, 74  
DISL, 69, 96, 101, 102, 106  
DISL BRIE, 98  
DISL BRIL, 97  
DISL BRIT, 97  
DIS LLB, 65  
DIS LSSL, 74  
DIS MSDL, 68, 83  
DIS MSDL ALL, 68  
DIS MSDL AUDM, 68  
DIS MSDL DBG, 68  
DISN, 98  
DIS PRT, 83  
DISR, 106  
DIS RLB, 65  
DISS, 96  
Distant Steering Code, 199  
DIS TEST, 65

DIS TTY, 83  
DISU, 94, 99, 108  
DISX, 106  
DIS ZBR, 111  
DIS ZONE, 111  
DNCK, 55  
DSC. *See* Distant Steering Code.  
DSCH, 70  
DSPL, 59  
DSPL ALL, 59  
DSPA, 98  
DSRB, 99  
DSXP, 98  
DSYL, 70  
DTR, 106

## E

Echo Servers for NAT, 155  
EDD, 215  
edit Bookmarks, 37  
Electronic Switched Network, 173, 197  
    Access Codes and Parameters, 199  
Embedded LAN, 143  
ENCH, 70  
ENCK, 55  
ENCL, 97  
ENCL BRIL, 97  
ENCL BRIT, 97  
ENL, 89, 104  
ENL AML, 46  
ENL AUTO, 65, 99  
ENLC, 94, 108  
ENLC BRI, 98  
ENL CC, 54, 55  
ENL CNI, 59

ENL DCH, 65  
ENL DDSC, 75  
ENL DDSL, 75  
ENL DTCS, 75  
ENL DTRC, 75  
ENL DTSL, 75  
ENL DTVC, 75  
ENL ELAN, 46  
ENL EXT, 59  
ENL FIL, 57  
ENLL, 70, 96, 97, 101, 102, 106  
ENLL BRIL, 97  
ENLL BRIT, 97  
ENL LLB, 66  
ENL LSSL, 75  
ENL MSDL, 68, 83  
ENL MSDL all, 68  
ENL MSDL AUDM, 68  
ENL MSDL FDL, 68  
ENLN, 98  
ENL PRT, 83  
ENLR, 106  
ENL RLB, 66  
ENLS, 96  
ENL TEST, 66  
ENL TTY, 83  
ENLU, 108  
ENLX, 106  
ENL ZBR, 111  
ENL ZONE, 111  
ENPS, 98  
ENRB, 99  
Enterprise Translations Server, 201  
ENXP, 98

ENYL, 70  
Equipment Data Dump, 215  
EREF, 55  
EST AML, 45  
EST DCH, 66  
Ethernet and Alarm Management, 115, 148, 152, 153, 155  
Ethernet Diagnostics, 75  
Ethernet Quality of Service Diagnostic, 79  
Event Default Table, 116  
Event Preference Table, 81, 116  
Exchange (Central Office) Code, 200

## F

FCAS. *See* Free Call Area Screening.  
FCR. *See* Flexible Code Restriction.  
FCTO, 118  
FDIS NCAL, 99  
FDL. *See* Force Download.  
FDLC, 99  
FDLU, 99  
feature options, 171, 172  
feature packages, 112, 175  
FFCS, 171  
file upload, 162  
firmware, 144, 162  
Fish, 23  
Flexible Code Restriction, 206, 211  
Flexible Feature Codes, 171  
Force Download, 90  
Free Calling Area Screening, 200  
Free Special Number Screening, 200  
FSNS. *See* Free Special Number Screening.  
FSUM, 99  
FWVU, 99

**G**

General Commands, 129  
General Options, 183  
Geographic Redundancy, 116  
GRTHR, 118

**H**

H.323, 145, 201  
H.323 Settings, 144  
Help, 250  
HLOC. *See* Home Location Code.  
HNPA. *See* Home Area Code.  
Home Area Code, 200  
Home Location Code, 200

**I**

ICOG, 180  
IDC, 55, 96, 97, 98, 99, 181  
IDC CNI, 59  
IDC CPU, 59  
IDCS, 98  
importing Node files, 140  
INC, 186  
Incoming Digit Conversion, 209, 211  
Incoming Trunk Group Exclusion, 199  
Input/Output Diagnostics, 82  
IP Line, 14, 130  
IP Line 3.0, 15, 224  
IP Line 4.0, 14  
IP Line application commands, 130  
IP Phones, 144, 162  
IP Telephony, 129  
IP telephony, 128, 136, 139  
IP Telephony card, 128  
IP Telephony Information, 128

IP Trunk 3.0, 201  
ISDN, 173  
ITGE. *See* Incoming Trunk Group Exclusion.

**J**

JOIN, 60

**L**

LAN, 143  
LAPW, 232  
LATEST, 135  
LBSY, 96  
LCNT, 70  
LD 02, 223  
LD 117, 76, 80, 110, 115, 148, 152, 153, 154, 155  
LD 135, 56  
LD 15, 170, 171, 172, 173  
LD 16, 179  
LD 17, 191  
LD 30, 101  
LD 32, 95  
LD 36, 61, 65, 108, 110  
LD 37, 65, 82  
LD 43, 215, 217  
LD 48, 65, 67  
LD 49, 211  
LD 54, 93  
LD 73, 196  
LD 86, 197, 199  
LD 87, 197, 199, 200  
LD 90, 197, 200  
LD 96, 65, 104, 105, 108  
LD 97, 113, 118  
LDIC, 108, 109  
LDID, 109

LDIS, 96, 101  
LENL, 102  
LIDL, 96  
Link Diagnostic, 67  
Links, 26  
Listed Directory Number options, 173  
LLBK FIL, 57  
LLBK IP, 57  
LMAX, 109  
LMNT, 96  
LNDS, 109  
LOC. *See* Location Code.  
Local Steering Code, 199  
Location Code, 200  
LOCK, 57  
Logging into Element Manager, 23  
log in, 23  
LOOP, 102  
Loop Timer, 193  
Loss and Level Plan, 15, 144  
Loss and Level plans, 146  
LOVF, 71, 109  
LSC. *See* Local Steering Code.

## M

maintenance, 80, 81  
Maintenance Commands for Zones, 109  
MAP AML, 45  
MAP DCH, 66  
Media Gateway 1000B, 14  
Media Gateway 1000S, 14  
Member Property Configuration  
    advanced, 187  
    basic, 185  
MFR, 106, 107

Microsoft Internet Explorer, 201  
MIDN, 94  
MISP, 97  
MREF, 55  
MSDL, 67  
MSDL Diagnostics, 89  
MTST, 94  
Multi-Del, 187  
Multifrequency, 91  
Multifrequency Signaling Diagnostics, 93

## N

NAS. *See* Network Attendant Services.  
NAT, 155  
NAT Echo Servers, 155  
NAT session time-out value, 156  
navigation tree, 25  
NCTL. *See* Network Control Parameters.  
Netscape Navigator, 201  
Network Address Translation (NAT), 155  
Network and Peripheral Equipment Diagnostic, 95  
Network and Peripheral Equipment Diagnostics, 95  
Network and Signaling Diagnostics, 101  
Network Attendant Services, 199  
Network Control & Services, 198, 199  
Network Control Parameters, 199  
Network Loop, 96  
Network Numbering Plan, 197, 201  
Network Numbering Plan menu, 13, 27  
Network Options, 182  
Network Routing Service (NRS), 27  
Network Routing Service home page, 204  
Network Speed Call Access Code, 200  
Night service options, 175  
Node ID, 129

---

nodes, 143  
    add new, 139  
    delete, 140  
    edit configuration, 139  
    import files, 139

Node Summary, 139

NPA. *See* Numbering Plan Area Code.

NRS  
    Guest access, 205

NRS Manager, 197  
    Administrator access, 204, 205  
    Monitor access, 204

NSCL. *See* Network Speed Call Access Code.

Numbering Plan, 198, 200

Numbering Plan Area Code, 200

NXX. *See* Exchange (Central Office) Code.

**O**

online Help, 250

Operational Measurement Report, 129

Operational Measurements Report, 136

OPT, 171

**P**

PAD Category, 193

Password, 231

Patch Bin, 164

Patching menu, 13, 28

PERR, 99

Personal Directory, Redial List, Callers List, 161

ping an IP address, 132

PINS, 163

PLIS, 163

PNNC, 181

POOS, 163

POUT, 163

Primary Rate Interface, 193

PRT AQOS, 80

PRT DNIP, 78, 79

PRT IPDN, 78, 79

PRT ZBW, 110

PRT ZDES, 110

PRT ZDP, 110

PRT ZESA, 111

PRT ZONE, 110

PRT ZQNL, 81

PRT ZQOS, 80

PRT ZTP, 111

PSTAT, 163

**Q**

QoS, 15, 143, 156

QoS Call Basis Threshold Parameters, 157

QoS Zone Basis Threshold Parameters, 157

Quality of Service, 156

Quality of Service (QoS), 15

Quality of Service (QoS), 143

Quality of Service Thresholds, 156

**R**

RAN, 109

RCNT, 70

RD, 134

RDGO, 133

RDHEAD, 133

RDOPEN, 133

RDS, 134

RDSHOW, 133

RDTAIL, 133

Report Utility, 129, 132

reset element, 129

- Restore from Backup Data, 218
- RLB. *See* Route List Block.
- RLBK FIL, 57
- RLS AML, 46
- RLS DCH, 66
- ROUT, 180
- route, 178, 180
- Route Data Block, 169, 179
- Route List Block, 199
- Route Properties, 178
- Routing Entry, 201
- RPED, 102
- RSET, 108
- RST, 89
- RST DCH, 66
- RST MSDL, 67, 83
- RSTR\_RULE, 117
- RTMB, 185
  
- S**
- Save node files, 139
- SBFS, 57
- SCPU, 60
- SDAM, 118
- SDCH DCH, 66
- SDTR, 106
- SEFT CC, 55
- SFTO, 118
- SHLF, 102
- SIGL, 185
- Signaling Server, 13, 128, 129, 132, 144
- Simple Network Management Protocol, 14, 115
- Simple Network Transfer Protocol (SNTP), 15
- SIP, 144, 145
- SIP Converged Desktop Service, 144
- SIP Gateway, 144
- SIP Re-direct Server, 144
- SIP URI DN Mapping, 144
- SLFT, 70, 89, 102, 104
- SLFT AML, 46
- SLFT MSDL, 67, 83
- SNMP, 14, 82, 115, 143
- SNMP alarm browser, 116
- SNMP traps, 115
- SNTP, 15, 143, 224
- software upgrade, 128
- Software Upgrade menu, 13, 27
- SOTS, 57
- Special Number, 200
- SPLIT, 60
- SPN. *See* Special Number.
- SSCK, 54, 55
- STAT, 69, 70, 71, 84, 89, 93, 94, 96, 97, 98, 99, 102, 104, 106, 108
- STAT AML, 45
- STAT CNI, 58
- STAT CPU, 56, 58
- STAT DCH, 65
- STAT DDCS, 73
- STAT DDSL, 73
- STAT DTCS, 74
- STAT DTRC, 74
- STAT DTSL, 74
- STAT DTVC, 74
- State Control, 116
- STAT ELAN, 45
- STAT FIL, 56
- STAT GR, 61
- STAT HEALTH, 60

- 
- STAT HEALTH AML, 60
  - STAT HEALTH ELAN, 60
  - STAT HEALTH HELP, 60
  - STAT HEALTH HW, 60
  - STAT HEALTH IPL, 60
  - STAT LINK, 84
  - STAT LINK IP, 76
  - STAT LINK NAME, 76
  - STAT LINK NODE, 76
  - STAT LINK SRV, 76
  - STAT LSRC, 74
  - STAT LSSL, 74
  - STAT LSVC, 74
  - STAT MAC, 56
  - STAT MEM, 56, 58
  - STAT MSDL, 67, 83
  - STAT MSDL full, 67
  - STAT NCAL, 99
  - STAT NEXT, 58
  - STAT NWK, 98
  - STAT PER, 98
  - STAT PRT, 83
  - STAT SERV, 65, 77
  - STAT SERV APP, 77
  - STAT SERV IP, 77
  - STAT SERV NAME, 77
  - STAT SERV NODE, 77
  - STAT SERV TYPE, 77
  - STAT TTY, 83
  - STAT VTRM, 99
  - STAT XSM, 84
  - STAT ZBR, 111
  - STAT ZONE, 111
  - STIP HOSTID, 77
  - STIP NODE, 77
  - STIP TERMIP, 77
  - STIP TN, 77
  - STIP TYPE, 77
  - STIP ZONE, 77
  - STRI, 186
  - STRO, 186
  - STRT, 75
  - submit, 29, 40
  - Superloop, 113
  - SUPL, 96
  - Syslog, 129, 134
  - SYSLOG#, 135
  - System Date & Time, 223
  - System Date and Time, 225
  - System Information, 231
  - System Information web page, 25
  - System Status, 40
  - System Status menu, 12, 26
  - System Timer, 193
  - System Utility, 213
  - System Utility menu, 13, 28
- T**
- TDS, 106
  - TEIT, 102
  - Telnet, 32
  - Terminal Proxy Server, 202
  - Terminal Session
    - add, 33
  - TEST, 48, 102
  - TEST 100, 66
  - TEST 101, 66
  - TEST 200, 66
  - TEST 201, 66

TEST CNI, 59  
TEST CPU, 59  
TEST GR, 61  
TEST IPB, 59  
TEST LCD, 59  
TEST LED, 59  
TEST SUTL, 59  
Threshold Set Block, 194  
Threshold Set Index, 194, 195  
Threshold Set Index, adding, 195  
Threshold Set Index, editing, 195  
time-out, 25  
TKTP, 180  
TMDI Diagnostics, 103  
Tone and Digit Switch Diagnostics, 105  
Tone and Digit Switch numbers, 112  
TRAC, 50, 52  
TRAD, 50, 53  
TRAK, 51  
Transfer/Status, 140, 142  
TRAO, 51  
TRAT, 50, 53  
TRCK, 55  
trunk, 178, 180, 184, 187, 188  
Trunk Data Block, 169  
Trunk Diagnostic, 108  
Trunk Diagnostics, 107  
Trunk Steering Code, 199  
TSC. *See* Trunk Steering Code.  
TTPM, 108  
TTSM, 102  
TTWI, 102

## U

UNLOCK, 57

UNTT, 102  
update, 29, 40  
UPLD AML, 46  
User Endpoint, 201

## V

VGWChannel, 140  
VGW Profile data, 143  
VIEW, 134  
Virtual Office Automatic Logout, 172  
Virtual Terminal, 129  
Virtual Terminal Session  
    Call Server, 33  
Virtual Terminal Sessions, 31  
VO\_ALO, 172  
Voice Gateway, 224  
Voice Gateway Media Card, 14, 15, 144

## X

XNTT, 96  
XPCT, 98  
XPEC, 98  
XRST, 96  
XTRK, 185

**Z**

Zone, 146

    Basic Property and Bandwidth Management,  
        147, 148

    Branch Office Dialing Plan and Access Codes,  
        147

    Branch Office Emergency Service  
        Information, 147, 153

    Branch Office Time Difference and Daylight  
        Saving Time Property, 147, 154

    Dialing Plan and Access Codes, 151

    Emergency Service Information, 153

    Time Difference and Daylight Saving Time  
        Property, 154

Zone Diagnostic, 55, 57

Zone Diagnostics, 109





Nortel Communication Server 1000

# **Nortel Communication Server 1000 Element Manager System Administration**

**Copyright © 1994–2008 Nortel Networks. All Rights Reserved.**

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

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

Publication number: 553-3001-332

Document release: Standard 5.00

Date: May 2008

To provide feedback or report a problem in this document, go to [www.nortel.com/documentfeedback](http://www.nortel.com/documentfeedback).

Sourced in Canada

