Nortel Communication Server 1000

System Management Reference

Release: 7.0
Document Revision: 04.02

www.nortel.com

NN43001-600

Nortel Communication Server 1000
Release: 7.0
Publication: NN43001-600
Document release date: 15 June 2010

Contents

New in this Release

The following sections detail what's new in *System Management Reference* (NN43001-600) for Release 7.0:

- "Features" (page 7)
- "Other changes" (page 7)

Features

See the following sections for information about feature changes:

Multi-user login

For Release 7.0 and greater, the overlay conflict resolution check is relaxed to allow Multi-User overlays to operate concurrently with LD 43, if only the database backup is performed on the Overlay.

For more information, see "Multi-User Login" (page 136).

Other changes

Revision History

June 2010	Standard 04.02. This document is up-issued to support Communication Server 1000 Release 7.0. Sections "Communication Server 1000 logs" (page 91) and "Patching Manager" (page 28) are revised.
June 2010	Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.0.

July 2009	Standard 03.04. This document has been up-issued to reflect editorial changes.
June 2009	Standard 03.03. This document is issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.02. This document is issued to support Communication Server 1000 Release 6.0.
December 2007	Standard 02.04. This document is issued to support Communication Server 1000 Release 5.5.
June 2007	Standard 01.03. This document has been up-issued to reflect changes in technical content which specifies that PDT access is required to access the Element Manager patching feature and adds a section on CS 1000 logging information.
May 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0 This document contains information previously contained in the following legacy document, now retired: *System Management (553-3001-300)*.
April 2006	Standard 3.01. This document is up-issued to support Communication Server 1000 Release 4.5. Updated with minor edits.
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, which resulted in the merging of multiple legacy NTPs. This new document consolidates information previously contained in the following legacy documents, now retired:

- XII System Management Applications (553-3001-301)
- Software Management (553-3023-300)

How to Get Help

Getting help from the Nortel web site

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

http://www.nortel.com/support

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

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

Getting help over the telephone from a Nortel Solutions Center

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

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

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

http://www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Introduction

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

Subject

This document describes the management interfaces and applications and their interactions available to Communication Server (CS) 1000.

Applicable Systems

This document applies to the following systems:

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

Intended Audience

This document is intended for individuals responsible for administering CS 1000 and Meridian 1 systems.

Conventions

Terminology

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

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

Related information

This section lists information sources that relate to this document.

Technical Documentation

The following technical documents are referenced in this document:

- *Unified Communications Management Common Services Fundamentals* (NN43001-116)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Element Manager System - Administration* (NN43001-632)
- *SIP Line Fundamentals* (NN43001-508)
- *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509)
- *Subscriber Manager Fundamentals* (NN43001-120)
- *Dialing Plans Reference* (NN43001-283)
- *Security Management Fundamentals*

  (NN43001-604)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Communication Server 1000 Fault Management - SNMP* (NN43001-719)
- *Software Input Output Reference — Maintenance* (NN43001-711)
- *Software Input Output Administration* (NN43001-611)
- *Software Input/Output: System Messages* (NN43001-712)
- *Patching Fundamentals* (NN43001-407)

Overview

Contents

This section contains the following topics:

Centralized management

OAM functionality is consolidated into the Unified Communication Management (UCM) environment (this includes functionality previously available in Telephony Manager (TM)).

The following Table lists TM functionality and describes the replacement functionality available in the UCM-based applications.

Table 1
TM functionality available in UCM applications

TM functionality	Alternative functionality in the centralized management environment
Telephone Administration (also referred to as Telephone Manager, Web Station, Station Admin)	Use the CS 1000 Element Manager (EM) **Phones** menu to provision phones on CS 1000 systems. Templates, reporting, bulk operations, CSV export/import, and so on are available in EM. Subscriber Manager works with templates in EM and CallPilot, which provides a common interface for provisioning CS 1000 phones and CallPilot mailboxes.
LDAP synchronization (through CND)	Subscriber Manager provides Lightweight Directory Access Protocol (LDAP) synchronization capabilities. The Common Network Directory (CND) is an embedded component (that is, UCM directory services) that is deployed as part of the UCM Common Services. The Subscriber Manager application includes a user interface to configure tasks such as LDAP synchronization, CSV synchronization, and CSV export.
Scheduling	Schedule LDAP synchronization jobs, as well as the addition and deletion of accounts using Subscriber Manager. Subscriber Manager includes an interface to view, edit, and delete scheduled jobs.
Corporate Directory	The Corporate Directory functionality is provided as a network-level application under the CS 1000 Services branch in UCM. The Corporate Directory application uses data from the Subscriber Manager and Numbering Groups applications to form a directory file consisting of names and phone numbers that is uploaded to CS 1000 systems and accessed by the phones. Corporate Directory and Numbering Groups applications are deployed with Subscriber Manager.
List Manager	Use the CS 1000 EM **Phones** menu to manage lists (Speed Call, System Speed Call, Group Hunt, and Group Call). Supported functionality includes: • single list configuration • retrieval of configured lists • CSV bulk import and export • deletion of single or multiple lists • refresh capability (lets you retrieve the latest data about list configuration)

TM functionality	Alternative functionality in the centralized management environment
Traffic Reporting	Use CS 1000 EM to display traffic reports. EM can display the historical traffic data, as well as the current data. Generated traffic-related data is collected from the call server at regular intervals (30 minutes) and stored in a database in the system where EM is running. You can enable or disable the traffic data collection. Use the PREV, NEXT buttons to display the historical reports in the traffic report pages. For additional functionality, such as generating “what-if” reports (used in capacity planning), consult Call Accounting vendors that also offer traffic reporting solutions.
Maintenance Windows	Use CS 1000 EM to perform maintenance commands.
ESN ART	Use CS 1000 EM to manage ESN data.
DECT Manager (TM Web DECT Application)	DMC DECT Manager is a standalone Windows®-based application.
Alarm Notification/ Alarm Viewer	Use Visualization, Performance and Fault Manager (VPFM) to perform fault consolidation within each site and to filter and forward faults to a central Network Management System (NMS), such as VPFM or a third-party solution. VPFM is a separately licensed UCM application.
Call Accounting, Traffic Analysis, Call Tracking, DBA (Data Buffering and Access)	Choose a supported third-party application to meet your needs. Avaya DevConnect Members that have Call Accounting and Traffic Analysis applications can provide a solution. For more information about Avaya Developer Partners, see: https://devconnect.avaya.com/

Hardware platforms and operating systems

Element Manager, Network Routing Service Manager, and Subscriber Manager are installed with the Nortel Unified Communications Management (UCM) Common Services on a Nortel CP PM server or on one of the following Commercial Off The Shelf (COTS) servers:

- Dell (R300)
- Hewlett Packard (HP DL320)
- IBM (IBM 360 or IBM 3550)

This deployment integrates the (UCM) Common Services security domain. Users can log on once and use Element Manager, Network Routing Service Manager, or Subscriber Manager.

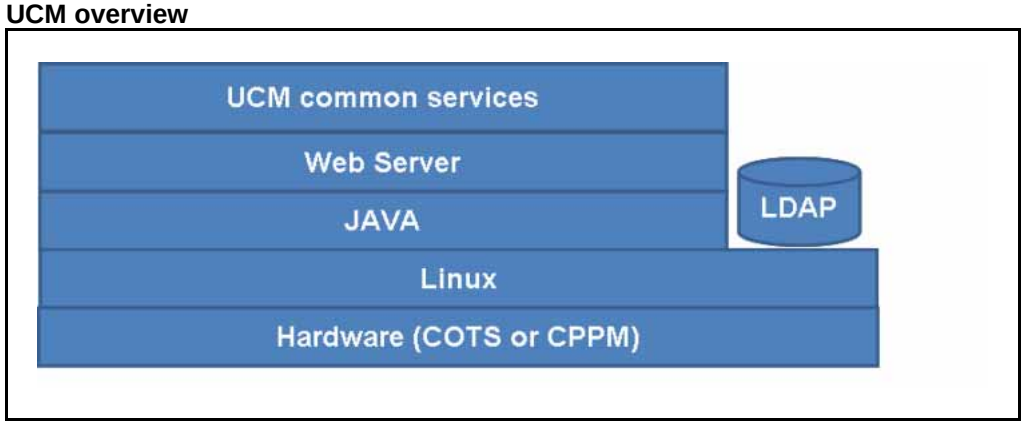
Unified Communications Management

Unified Communications Management (UCM) is a collection of system management tools. UCM provides a consistent methodology and interface for performing system management tasks. System management tools are web-based system management solutions supported by the UCM framework.

Installed on every Linux OS, is a web server with extended security features. This forms the bases for UCM and provides the following key features.

- Central element registry for all elements
- Authorization and authentication functionality
- Single sign on across application and hardware platforms
- PKI management
- Radius support
- External authentication support

Figure 1
UCM overview

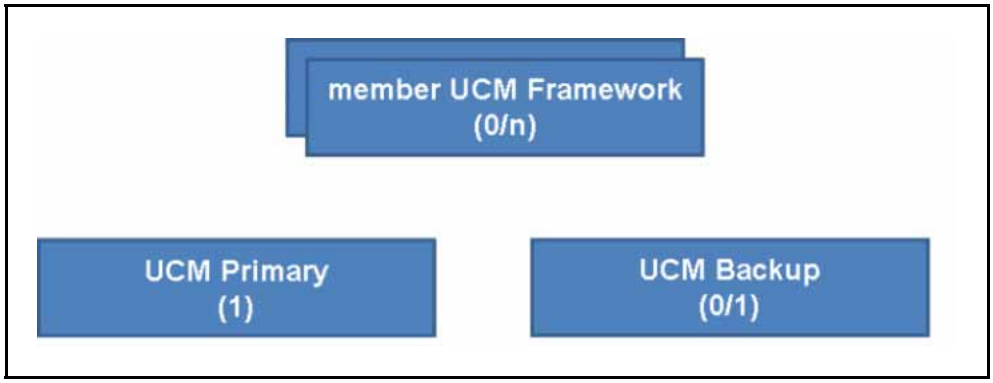


You can configure UCM in one of the following ways:

- Primary security server
- Backup security server
- Member security server

Every security domain must have 1 primary security server. The security domain can have 0 or 1 backup servers; any additional servers are member servers.

Figure 2
UCM server configurations



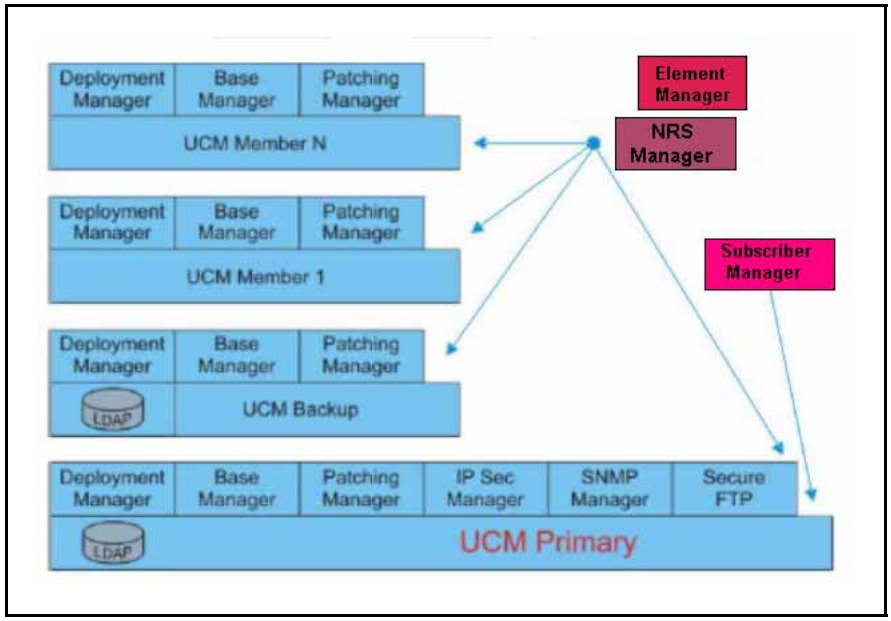
UCM framework is installed and run on all CS 1000 Linux platforms (CP PM and COTS). Management applications are packaged as Web Archive (WAR) files and load into the UCM framework.

CS 1000 management applications are auto-deployed, other management applications are deployed as required.

- Auto-deployed to the UCM server
  - Base Manager: Provides local web management for Linux base.
  - Deployment Manager: Enables application installations and upgrades. Deployment Manager can be accessed centrally from the Primary security server or locally on the target server.
  - Patching Manager: Provides web based patch delivery. Patching Manager can be accessed centrally from the Primary security server or locally on the target server.
  - IPSec Manager: Provides centralized web based IPSec management.
  - SNMP: Provides centralized web based fault management.
  - Secure FTP: Provides centralized web based SFTP.
- User deployed
  - Element Manager: Provides traditional CS 1000 web based management, including Call Server overlay support.
  - Network Routing Service Manager
  - Subscriber Manager

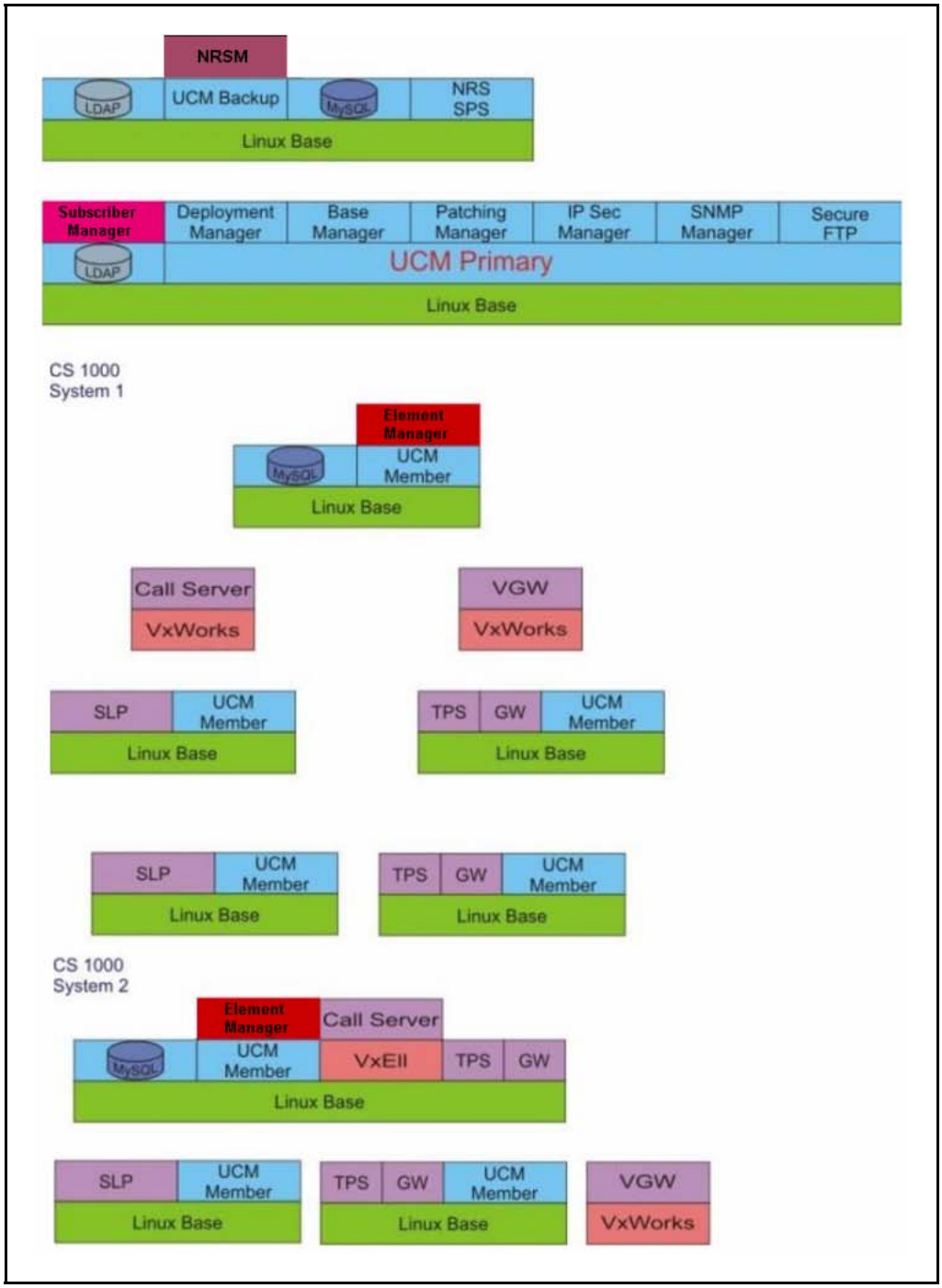
The following figure provides a graphical representation of applications deployment on UCM servers.

Figure 3
UCM application deployment



The following graphic provides an example of system management components deployed in a typical installation. Network and engineering analysis determines the location of the UCM primary and backup servers. Typically EM is deployed physically close to the Call Server it is managing.

Figure 4
Physical deployment of UCM



The UCM Graphical User Interface (GUI) is shown in Figure 5 "UCM graphical interface" (page 22).

Figure 5
UCM graphical interface

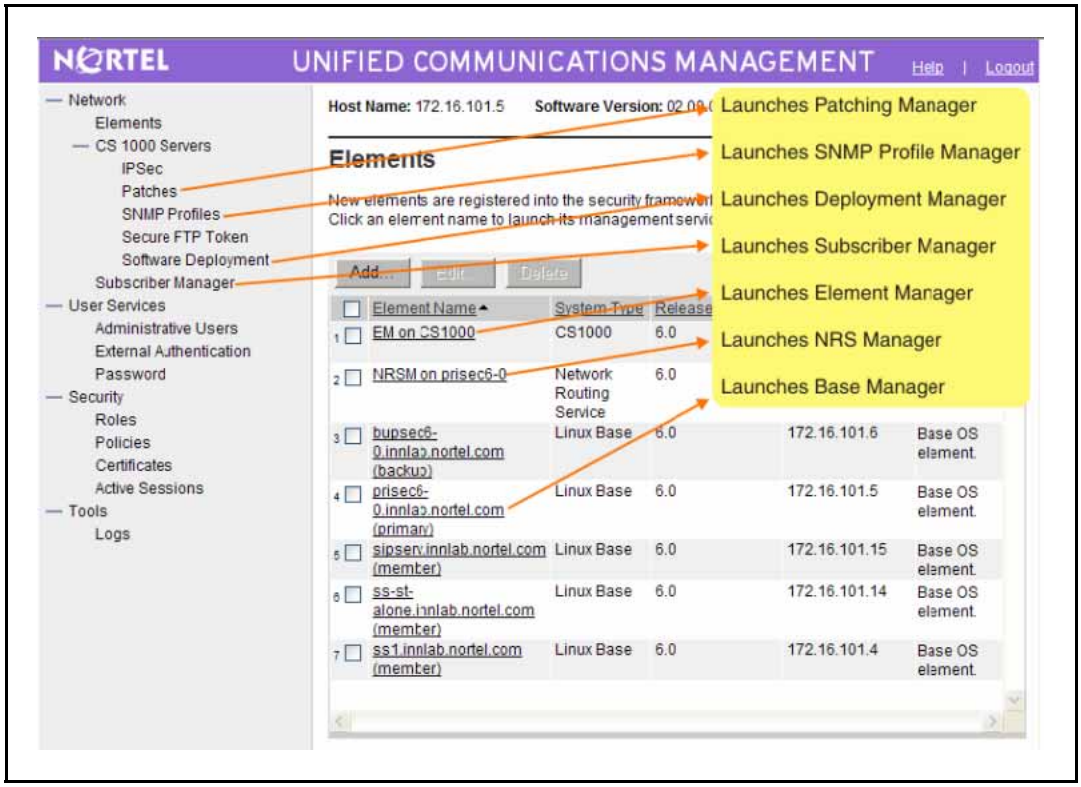
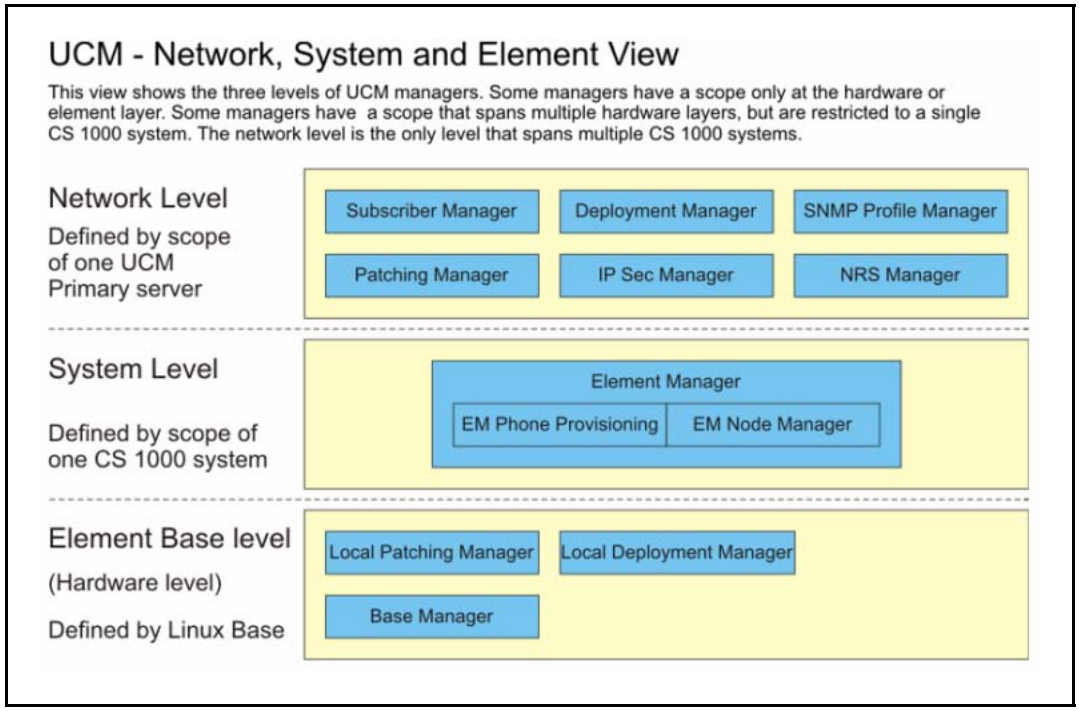


Figure 6 "UCM management levels" (page 23) shows the 3 levels of UCM managers.

Figure 6
UCM management levels



For information about the components, features, and benefits of Unified Communications Management, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Element Manager

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

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

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, check boxes, and range values to simplify response selection.

Access to Element Manager is through the Unified Communications Management (UCM).

The following management tasks are performed using Element Manager:

- Links: Provides access to Virtual Terminal sessions.
- System: Provides access to system-wide configuration and basic hardware/software management, including supported maintenance overlays and configuration.
- IP Network: Helps the user access all functions related to managing IP Networks. 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.
- Phones: Enables users to configure phones for the Call Server.
- Dialing and Numbering Plans: Configures all Electronic Switched Network (ESN) data blocks for the Call Server.
- Tools: Provides general administrative tools, features, and functions, and allows the user to find and access task-related pages, including Reports.
- Security: Allows the user to perform Security functions, including IP Security.

Element Manager is installed on UCM. Element Manager uses UCM logging facility, including the log viewer interface, the security framework, and the Web server. Each UCM is installed with specific requirements for hardware platforms and operating systems that are applicable to Element Manager.

Users access UCM and Element Manager through Microsoft Internet Explorer 6 or later.

The UCM is deployed on a Nortel CP PM server or on a selected Dell, IBM, or Hewlett Packard Commercial Off The Shelf (COTS) server.

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

Network Routing Service Manager

Use Network Routing Service (NRS) Manager, a web-based management application, to configure, provision, and maintain the NRS.

The SIP Proxy NRS resides on a COTS server that hosts Unified Communications Management (UCM).

NRS includes both the H.323 Gatekeeper and SIP Redirect/Registrar Server. The NRS provides routing services to both H.323- and SIP-compliant devices.

NRS Manager allows users to manage a single network dialing plan for SIP, H.323, and mixed H.323/SIP networks. The user can configure the H.323 Gatekeeper application for routing services for H.323 endpoints and the SIP Redirect Server for SIP routing services.

Element Manager and NRS Manager are closely linked. Element Manager must be used to enable the SIP Redirect Server and/or H.323 Gatekeeper and to configure the role of the NRS to access NRS Manager.

For detailed information about the NRS and NRS Manager, see *Network Routing Service: Operations (NN43001-564)*.

Subscriber Manager

Subscriber Manager is an intuitive and user-friendly Web-based interface that is deployed as a plug-in application to the Unified Communications Management (UCM). Subscriber Manager provides a centralized location for the management of subscriber information for enterprise services.

With Subscriber Manager, you can:

- easily manage subscribers and accounts (i.e. phones) within your network
- quickly search, sort, and update single and multiple subscribers and subscriber accounts within a single application interface

Prior to Subscriber Manager, subscribers and accounts were managed by individual element managers or element management systems. Subscriber Manager eliminates the need to configure and manage separate subscriber management applications for specific products in a management system.

Subscriber Manager leverages UCM for security and user access control and provides simplified management tasks, and improved workflow efficiency."

Subscriber Manager components

The Subscriber Manager plug-in application is installed on UCM. Subscriber Manager uses UCM logging facility, including the log viewer interface, the security framework, and the Web server. Each UCM is installed with specific requirements for hardware platforms and operating systems that are applicable to Subscriber Manager.

Users access UCM and Subscriber Manager through Microsoft Internet Explorer 6 or later.

The UCM is deployed on a Nortel CP PM server or on a selected Dell, IBM, or Hewlett Packard Commercial Off The Shelf (COTS) server.

The Subscriber Manager application is installed with the UCM from the UCM DVD using the Deployment Manager. Subscriber Manager co-resides with Element Manager when deployed.

You can access various functions to manage subscribers and accounts within a network. The Subscriber section in the UCM navigation tree contains the following links:

- Subscribers - Use this link to perform the following tasks:
  - search for subscribers
  - view and update subscriber information
  - add a new subscriber
  - delete a subscriber
  - add or delete a subscriber account
  - view and update subscriber phone properties
- Synchronize Accounts: Use this link to synchronize account information between Subscriber Manager and elements and to assign or delete orphaned accounts.
- Flow through Provisioning (FTPROV): Allows customers to use their LDAP data store to drive account creation in Nortel products. FTPROV

replaces the Subscriber Change Notification feature in Subscriber Manager 1.0.

- Numbering Group: A numbering group represents common numbering planning attributes which are shared by a group of subscriber telephony accounts. Each telephony account can belong to only one numbering group. If a telephony account does not belong to a specified numbering group, it is classified as a member of the default numbering group category. A member of the default numbering group category only uses a private numbering plan (private CDP and UDP dialing).
- Locations: Used to manage locations within your network.

For more information about Subscriber Manager, see *Subscriber Manager Fundamentals* (NN43001-120).

Deployment Manager

The centralized Deployment Manager is responsible for deploying software applications from a central location. Every Linux server that is installed on the network is learned by UCM Common Services where the centralized Deployment Manager is running. The centralized Deployment Manager picks up these servers and initiates a remote software deployment from within UCM Common Services. The Service Cluster management interface adds the servers to a cluster from the list of servers that UCM has learned. Prior to adding the servers to a cluster, the Centralized Deployment Manager feature deploys the necessary software application to each of the Linux servers.

The Deployment Manager Web page opens allowing you to select the following:

- Deployment Target
- Software Loads
- Backups

For information on the procedures for backing up, restoring, or deploying software, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Base Manager

Base Manager is part of the UCM solution. You must log on to Unified Communications Management (UCM) to perform configuration procedures using Base Manager. For more information about Base Manager refer to, *Unified Communications Management Common Services Fundamentals* (NN43001-116) and *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Patching Manager

Patching Manager (PM) is a centralized patch deployment application.

Patching Manager is available at two levels:

- Centralized PM runs on a Primary UCM server to provide patching support for all the Linux Servers in the same security domain; for example, Primary, Secondary and Member servers under the same security domain. PM gets the list of all elements that can be patched from UCM. The link for the Certralized PM is included in the UCM navigator menu.
- Local PM can be accessed from Base Manager of each Linux base element. PM provides patch management support through central UCM logon and local logon

Patching Manager for Communication Server 1000 provides the following:

- Binary patching support
- Loadware support
- Deplist support
- Linux Call Server (VxELL) patching support
- Enhanced Linux service pack support
- High Scalability support
- Enhanced color coding to indicate user actions, warnings, and errors

For detailed information about the Patching Manager, see *Patching Fundamentals* (NN43001-407).

Command Line Interface

The Command Line Interface (CLI) is a character-based serial interface to the operating system and overlay programs on each system component.

The CLI administration programs implement and modify system features and reflect changes in system configuration. For example, the system administrator uses administration programs to make changes to directory numbers, telephones, trunks, and features.

Administrative and maintenance programs load in response to an instruction from the Call Processor or to a command from a system terminal or maintenance telephone. Because of how they load, the programs are referred to as overlays. For more information about the programs, see “System reporting” (page 86).

After loading, the administration programs use a step-by-step prompt/response format. The program issues a prompt for input; the system administrator enters the appropriate response by using the keyboard, then presses the **Return** key. The **Return** key (represented in procedures as <cr>) signals the end of each response.Table 2 "Using an administration program" (page 29) shows an example of prompts, responses, and descriptions of each.

Table 2
Using an administration program

Prompt	Response	Description
REQ	CHG	The program requests input; the response indicates the need to change some data.
TYPE	CFN	The program asks for the type of data to change; the response indicates that the data is in the Configuration Record.
PARM	YES	The program asks if the change is to a system parameter; the response confirms that it is a change to a system parameter.
- ALRM	YES	The program asks whether to enable the minor alarm on attendant consoles; the response confirms that the alarm is to be enabled. This alarm is under the category of a parameter, that is, PARM.
REQ	****	The program prompts for more input; the response ends the program.

If the response is valid, the system program issues the next prompt. If the response is invalid, the program issues a message using the format SCHxxxx, where SCH stands for Service Change, and xxxx is the specific message identifier. For an explanation of each SCH message, see "System messages" in *Software Input/Output: System Messages (NN43001-712)*.

All prompts and responses, commands, and system messages for the CS 1000 and Meridian 1systems are in the following NTPs:

- *Software Input/Output: Administration (NN43001-611)*
- *Software Input/Output: System Messages (NN43001-712)*
- *Software Input/Output: Maintenance (NN43001-711)*

Procedures in the document library generally contain short implementation tables to document the commands that are necessary to implement a feature or action.

Communicating with the system

Contents

This section contains the following topics:

Introduction

Users can communicate with the system using Input/Output devices such as maintenance workstations, maintenance telephones, RS-232 Video Display Terminals (VDTs), teletypewriters (TTYs), and printers (PRTs).

The supported devices are as follows:

- Maintenance workstation
  - — equipped with a dial-up modem or connected to the network
  - — equipped with a terminal emulator application such as Telnet or rlogin
  - — equipped with a web browser
- Maintenance telephone, for certain maintenance and testing activities. For more information about the Maintenance Telephone,

see *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)*.

- Maintenance terminals (VDTs and TTYs) with a serial connection to the Call Server, Media Gateway, Signaling Server, or Voice Gateway Media Cards.

Data communication technologies

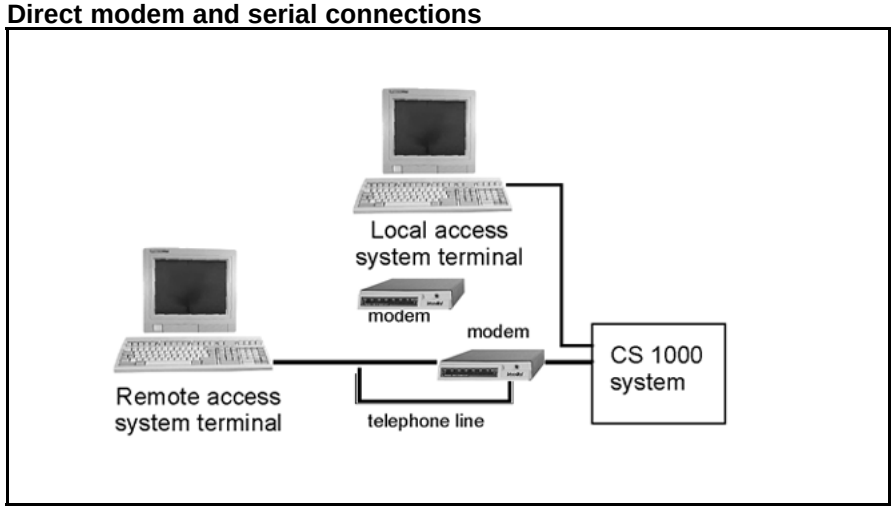
Access each component through an RS-232 maintenance port. Locally, users can connect a maintenance workstation to the RS-232 port, which can require a null modem adapter.

Ports that can establish a Point-to-Point Protocol (PPP) link use dial-up modems. This protocol is used for communication between two computers, using a serial interface. A single device connection is robust and simple, but a central connection point promotes ease of use. The following methods promote central access to a varying degree:

- Modem on the Call Server or Signaling Server with PPP link for Telnet applications and web access for normal operations (not emergency maintenance) to enable access to the Embedded Local Area Network (ELAN) subnet
- Modem router on the ELAN subnet
- Terminal server
- Secure dial-up Remote Access Server (RAS)
- Virtual Private Network (VPN) access to the enterprise network over the Internet

The ideal solution is to implement reliable dial-up access to a central server or network, where you can use Telnet to connect through a terminal server to individual components on the ELAN subnet, and, therefore, to obtain maintenance access on each device. Figure 7 "Direct modem and serial connections" (page 33) illustrates direct modem and serial connections.

Figure 7
Direct modem and serial connections

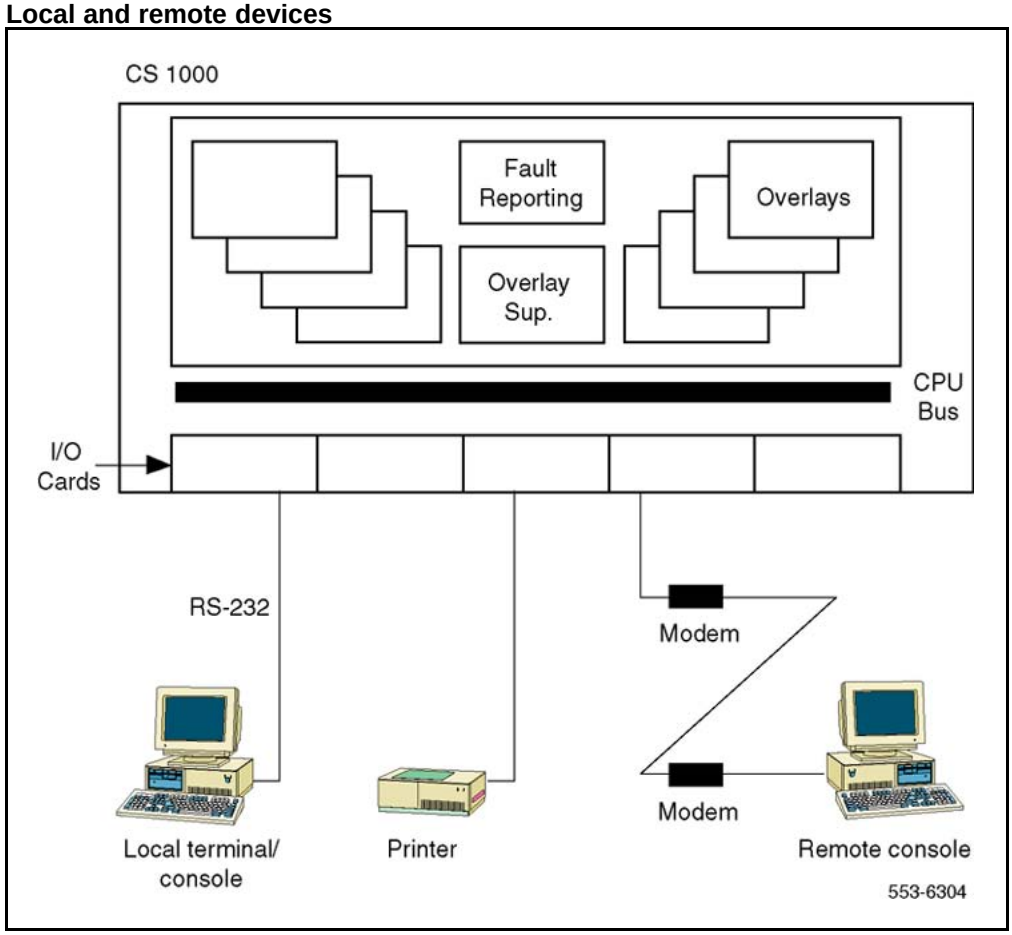


Local and remote access

Input/output (I/O) terminals can operate either locally or remotely. For local or remote access, maintenance terminal connections access components through a terminal server, modems, and over the Telephony LAN (TLAN) or ELAN network interface. Strictly local access occurs over a serial cable that connects directly to the component in question.

A device within 50 feet of the central control unit is a local device that connects directly to a Serial Data Interface (SDI) card. A device more than 50 feet from the central control unit is a remote device and must connect to the SDI card through modems and a telephone line. See Figure 8 "Local and remote devices" (page 34).

Figure 8
Local and remote devices



Local serial connections

Serial connections enable access to an element Command Line Interface (CLI).

Call Server

To access the Call Server, a Media Gateway, or an MG 1000B Core over a serial connection, consult *Software Input/Output: Administration (NN43001-611).* Alternatively, see *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)*.

Signaling Server

To access the Signaling Server over a serial connection, refer to *Signaling Server IP Line Applications Fundamentals (NN43001-125)*. The CLI is intended for advanced maintenance.

Circuit cards

Each circuit card is described in the *Circuit Card: Description and Installation (NN43001-311)*.

Remote serial access

Call Server

The Call Server supports modem connections for serial maintenance terminal access or the establishment of a PPP link for IP communication.

To configure IP addresses for PPP, use LD 117, Ethernet and Alarm Management. For more information, refer to LD 117 in *Software Input/Output: Maintenance (NN43001-711)*.

Signaling Server

Remote access to the system is possible with a modem connected to the Signaling Server maintenance port and using a PPP link for IP communication.

Alternatively, remote access is possible with an RAS modem router installed on the ELAN subnet.

Connect a modem to the Signaling Server and dial into it. Once connected, use the Signaling Server CLI. Initiate a PPP session to access the Element Manager web page on the browser. From there, use Telnet to connect to the Voice Gateway Media Cards.

If the Signaling Server experiences a problem, and the user needs to connect remotely as part of a troubleshooting scenario, then the above connection cannot work. In anticipation of this scenario, connect multiple modems to the various serial ports of the Signaling Server, Voice Gateway Media Cards, Call Server, and Media Gateway. Connect multiple modems to dial into a port on the component that requires troubleshooting. This approach for each system component is not practical or cost-effective as it requires the site to use multiple modems with multiple telephone lines.

A better option is to use a modem with a router, a modem router, a terminal server, or combination of the three. These devices provide serial interfaces to connect to the various ports and a dial-up interface for remote connection. These devices also include an Ethernet interface to remotely connect to the device using Telnet and, from there, use Telnet or rlogin to access the various system components. For information about how to install a modem router on the system, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125). A terminal server is similar to a modem router, but has 8 to 12 RS-232 serial ports that are cabled to individual components.

Maintenance connectivity for distributed components (not co-located) can require full nine-pin serial cables between the server, the element, and the workstation for optimal performance.

Network connections

To access the Call Server, Media Gateway, Signaling Server, and Voice Gateway Media Card over the TLAN or ELAN network interface, connect to the network as described in *Communication Server 1000E: Installation and Configuration (NN43041-310)*. The data network connection is through a Layer 2 switch on the network.

To access Element Manager and Network Routing Service (NRS) Manager on Linux, connect to Unifed Communication Management (UCM) as described in *Unifed Communication Management - Fundamentals* (NN43001-116), and *Network Routing Service: Operations (NN43001-564)*.

To limit access to system components and all devices on the customer data network, comply with all the usual security precautions, many of which are described in “Security” (page 72). If possible, use an access list on the routers, so that only certain users or ports can access the ELAN subnet, TLAN subnet, or both.

Because system login authentication is always an aspect of security, refer to “Security” (page 72) for pertinent information.

Element Manager web interface

A computer with a web browser is required to access Element Manager through the UCM network interface.

The management workstation is on t a TLAN subnet, or have access to the TLAN subnet (for example, through a router or a switch on the customer data network). For more information about switch connections, see the *Converging the Data Network with VoIP (NN43001-260)*.

Subscriber Manager

The UCM security domain provides the launch point for Subscriber Manager. You can access Subscriber Manager when you log on to the UCM framework or through a direct Web link. When Subscriber Manager is installed in the UCM framework, the Subscriber link is provided in the left pane of the UCM navigator. You can also launch Subscriber Manger by navigating to the **Network > Services** Web page of UCM.

For more information see, *Unified Communications Management - Fundamentals* (NN43001-116).

I/O port lockout

The system software has an I/O port lockout mechanism to help prevent the TTY and PRT devices from impairing system performance.

When the system detects excessive interference or a burst of invalid characters on a TTY or PRT port, the system locks the port. An automatic recovery mechanism re-enables the port after 4 minutes. If more than three lockouts occur within 30 minutes, the port is disabled and a system message is issued. If this occurs, a technician must manually re-enable the port.

Point-to-Point access

The system has ELAN network interfaces and supports Transmission Control Protocol/Internet Protocol (TCP/IP). Point-to-Point Protocol (PPP) is an asynchronous implementation of the standard data link level PPP included in the Internet protocol suite. This function provides a common network interface for applications that use the TCP/IP stack for remote system access.

Operating parameters

Although one feature of PPP is to support various network layer protocols in the system client-server environments, only TCP/IP protocol is supported. This limitation does not alter the standard PPP implementation to prevent future support for other protocol stacks.

Though the PPP protocol supports both synchronous and asynchronous data communication, support is available only for asynchronous data links.

Only one active PPP link can be established at a time to minimize the impact to the CPU and memory usage by the amount of networking traffic from PPP and Ethernet.

Because of the various ways the data bits are used between PPP (8 bits) and system overlays (7 bits), the system port must use 8 data bits to satisfy the PPP protocol requirement. Because the system always sets the most significant bit (eighth bit) to "1", the receiving terminal must reset its terminal to mask the eighth bit when communicating to system overlays.

System components

The system access and networking components include the existing system overlay. Support exists for three types of remote connections are supported:

- Normal SDI interface to system overlays (current)
- Normal SDI with Serial Line Internet Protocol (SLIP) session through Problem Determination Tools (PDT) (current for field support only)

The PPP implementation uses LD 137 with the **`pppBegin`** command to start the PPP links.

Description

PPP provides a standard encapsulation scheme to transmit IP datagrams over a serial link. The advantage of this scheme is to simplify the network access for system client/server applications. The server and client applications can communicate with each other through their IP addresses regardless of the type of data links available for datagram transmission.

Serial Port Interfaces

Only asynchronous links are available to establish PPP links on SDI hardware-supported systems.

SDI ports For asynchronous PPP links, support is available for any physical SDI port configured on the system with USER type MTC (Maintenance) or SCH (Service Change). PPP provides communication interface to the system application to perform administration and maintenance tasks. Therefore, the user must configure the system SDI port used for the PPP link to MTC /or SCH. Other USER types associated with MTC or SCH are considered valid SDI ports for a PPP link.

Port communication parameters PPP works in full-duplex communication and at various speeds. The following are the required configurations for the system:

- baud rate is limited to the type of hardware the SDI port can provide
- eight Data bits, one Stop bit
- no parity
- transmission mode set to DTE
- standard RS-232C interface

Configure the SDI port to eight data bits. For applications that need to configure an active TTY session through the same serial connection, the user must configure the terminal emulation program to ignore the eighth bit to avoid garbage characters on the terminal screen when they access the system overlay.

The performance of a PPP link is based on the baud rate of the physical asynchronous connection. Although the baud rate of the system SDI hardware support can be as low as 300 bits per second (bps), this connection speed does not work for many TCP/IP network services. A typical PPP link should run at 9600 bps to obtain a reasonable throughput.

Modem configuration

Before a modem connects to the system serial port, the user must correctly configure the modem with an external terminal. Save the modem configuration in the internal battery-backed memory of the modem to protect against power failure.

PPP link establishment

The implementations of PPP links over the system PBX require special treatments to work under operating systems.

The physical-level connection is not part of the PPP links process. The physical-level connection, a direct line or modem dial up, must be established before the PPP link is initiated.

In-Bound PPP link establishment

For access (direct or remote) through a serial port on the system, the user must directly connect the TTY port to a system input or the overlay supervisor (idle state) when the serial link is established. After the physical serial connection to the system is established, the user can invoke the PPP link by issuing the pppBegin command. The pppBegin command loads the PPP protocol and starts the PPP Link Control Protocol (LCP) in establish state. If the LCP fails, the PPP link is disabled and control is returned to the overlay supervisor (idle state). You can automate this login process by using a script file that runs on the remote access station.

Out-Bound PPP link establishment

After the connection is made, the software starts the PPP handshaking process (pppBegin) and establishes LCP, PAP, and NCP as required.

PPP link termination

A PPP link terminates when a request (pppEnd) from an application is received or when an optional timeout due to inactivity on the link occurs. A disconnected modem call or direct link cannot trigger the link to go down because the system serial drivers do not monitor the RS-232 pins and cannot notify the upper layer applications when the port states changes. If this condition occurs, the optional idle timer times out and tears down the PPP link.

PPP link Access Log

The PPP link connection log records all the previous PPP links activities as messages. This RPT log file is maintained for system logging purposes only, and can be read only from the PDT shell with the RPT commands.

Operation

System configuration requirements

PPP is a link layer software protocol that handles data packets between the physical transmission and networking layer software. Before a PPP link can be established, the following conditions must be met:

- The system IP layer must be configured correctly in LD 117.
- A valid operational TTY port must be available.

- A PPP configuration file must be configured in LD 117.
- The user must configure modem connections and establish an active connection.

Configuring the network

The following serious problems can occur when the system core connects directly to a customer LAN:

- Broadcast packets can arrive when the system core is busy handling the data network traffic. This can degrade performance.
- Unauthorized access to the LAN. A direct LAN connection provides access to all the workstations on the LAN. With the correct user name and password, a user can access system core data through the login or FTP connection.

To protect the system core from LAN traffic and unauthorized access, Nortel recommends an external router to shield the system core from the enterprise IP network and to block unauthorized access.

If the system switch connects to a customer LAN, users need not configure the IP network; use the factory default setting instead. Otherwise, the user must configure various network database files and system startup files before the TCP/IP network can be used.

SDI Configuration

The TTY port configured in LD 117 must have user type MTC or SCH for a PPP connection. Ports configured as HSL (ACD/D High-Speed AUX link), ACD (Automatic Call Distribution printer for reports), and others cannot be used for PPP links. A technician must validate the port communication parameters before the user can enable the port for service; the PPP software cannot change the SDI port communication parameters configured in LD 117.

Due to the overhead of network traffic, configure the SDI port baud rate at 9600 bps or higher to increase the network throughput.

PPP configuration file

The PPP configuration file provides the PPP link manager with information about how the PPP code must run. Depending on the PPP implementation, the format of the configuration is different from one implementation to another.

Modem configuration consideration

PPP provides remote access through a modem connection. Because of the high overhead associated with the networking protocol data frames, a high-speed modem is required to achieve a reasonable data throughput. Also, because the serial driver cannot monitor the RS-232 pins and the SDI port is set to a configured baud rate, the software driver cannot detect the baud rate at which the modem is established. As a result, the user must fix the baud rate between the SDI port and the modem.

Nortel strongly recommends a high-speed modem with fixed/variable speed DTE interface to ensure that the baud rate between the SDI port and the modem is set higher than the actual link rate, thereby enabling maximum efficiency and throughput.

Operating parameters

Sysload

The active TTY port that runs a PPP session terminates when sysload occurs. The physical TTY port can be interrupted due to the sysload; the TTY port should remain enabled after the sysload. Re-establish the PPP links after the system sysload.

System initialization

When system initialization (INIT) occurs during an active PPP session, the PPP links are disabled. The associated TTY port remains active.

PPP under remote access environments

When applications remotely access the system, a PPP link is used to interface to the remote application on the system core. If the remote operating system is under heavy load (such as multiple applications running and busy processing system tasks) and in a high baud rate situation, the operating system may not service the interrupt from serial input before the next character arrives. As a result, characters can drop from the Universal Asynchronous Receiver/Transmitter's (UART) receive buffer.

When the preceding conditions occur, the remote system must replace its existing port equipped with 8250/16450 UART with the improved 16550 UART to relieve the CPU of interrupt overhead and allow greater latency time in interrupt servicing. The current 8250 or 16450 UART serial port works if the remote access system is not under heavy load.

For a high-speed PPP link (9600 bps or higher), Nortel recommends the 16550 UART.

Ns26550 ensures a reliable high-speed serial link in a Microsoft Windows environment. The 8250 or 16450 UART work in most current PCs in Microsoft Windows at a lower baud rate. However, at a speed of 9600

baud or higher, the serial interrupt may not get serviced in time by the Windows software, and the 8250 and 16450 UART have insufficient buffer reserved to store an input character before it is overwritten by the next input character. The 16550 UART is an improved version with additional buffer space for input characters.

Physical link interruption

Because a PPP link cannot monitor the state of the physical serial connection, a disconnected line or a dropped modem connection cannot terminate the active PPP link until the PPP link idle timer expires. If this happens, reconnect the serial cable or the modem connection before the idle timer expires, or reconnecting the line or replacing the modem cannot re-establish the PPP links.

Service change

Table 3 "LD 117: Service change" (page 42)lists the commands associated with a service change.

Table 3
LD 117: Service change

Prompt	Response	Description
=>	NEW HOST hostname IP address	Configure a new host entry
=>	NEW ROUTE network IP gateway IP	Configure a new routing entry
=>	CHG ELNK ACTIVE hostID	Change active Ethernet interface address
=>	CHG ELNK INACTIVE hostID	Change inactive Ethernet interface IP address
=>	Change PPP LOCAL hostID	Change local PPP interface address
=>	CHG PPP REMOTE hostID	Change remote PPP interface address
=>	CHG MASK nnn.nnn.nnn.nnn	Change subnet mask
=>	CHG PTM nnn	Change PPP idle timer
=>	OUT HOST nn	Remove a host entry from database
=>	OUT ROUTE nn	Remove routing entry from database
=>	RST MASK	Reset subnet mask to default
=>	RST PTM	Reset PPP idle timer to default
=>	RST ELNK ACTIVE	Reset active Ethernet interface to defaults
=>	RST ELNK INACTIVE	Reset inactive Ethernet interface to defaults
=>	RST PPP LOCAL	Reset local PPP interface to default

Table 3
LD 117: Service change (cont'd.)

Prompt	Response	Description
=>	RST PPP REMOTE	Remove remote PPP interface
=>	PRT ELNK	Print Ethernet interface address(es)
=>	PRT PPP	Print PPP interface address(es)
=>	PRT HOST	Print configured host entries
=>	PRT ROUTE	Print configured routing entries
=>	PRT MASK	Print subnet mask
=>	PRT PTM	Print PPP idle timer
=>	UPDATE DBS	Rebuild INDET.DB and renumber host and route entry ID

Configuration procedures

To ensure a successful PPP connection, the system core must be configured correctly. If the core is not connected to a customer's data network through either Ethernet or PPP, the factory default settings are used. Otherwise, the core must be configured to match the customer's data network requirements.

System Core without LAN access

No configuration is required if the core is not connected to the customer's LAN. Only Nortel applications can access the PPP and Ethernet.

System Core with LAN access

For customers who want to connect the system to their LAN, Nortel recommends an IP gateway or router to isolate data network traffic and to protect the core. The advantage of connecting the core to the customer's LAN is that the application software can be installed and can run on the customer's existing networked systems to take advantage of the network access and resources. Only Nortel applications can connect to the network.

Before the system core connects to a customer's LAN, the system networking layer software must be properly configured. All networking configuration must be done through LD 117.

To configure the system networking layer, perform the following actions:

- Obtain IP names and addresses from the network administrator, and use LD 117 to change the default system IP addresses to the new IP addresses, including the active and inactive Ethernet interface

addresses and local or remote PPP interface addresses. For a dual CPU setup, obtain two Ethernet interface IP addresses.

- Obtain the subnet mask from the network administrator, and configure the subnet mask using CHG MASK in LD 117.
- Obtain network host names and addresses from the network administrator, and add the host names and addresses through LD 117 "NEW HOST."

For the system core to send an IP data frame, routing information must be available for any gateway it needs. Each network route includes the destination network address and the gateway address. The gateway is used to forward the IP data frame from the core to the destination network. These IP addresses can be obtained from the network administrator.

To configure the network and gateway addresses, perform the following actions:

- Obtain the gateway/router address, and the network addresses, and use LD 117 "NEW ROUT" to add the network and gateway addresses. Verify that the gateway address is in the host table.
- Configure the PPP idle timer in LD 117 with "CHG PTM nnn". To simplify PPP's mode of operation, the only configurable run time parameter is the idle timer. The idle timer can be configured in LD 117 to disconnect an active PPP link after the idle timer expires.

Diagnostic and maintenance programs

Table 4 "LD 117: Maintenance PPP" (page 44) lists the Maintenance PPP commands available in LD 117.

Table 4
LD 117: Maintenance PPP

Prompts	Commands	Description
=>	ENL PPP	Enable PPP access; this enables PPPD
=>	DIS PPP	Disable PPP access; disable PPPD
=>	ENL HOST n	Add a host to run time host table
=>	DIS HOST n	Remove a host from run time host table
=>	ENL ROUTE n	Add a route to run time routing table
=>	DIS ROUTE n	Remove a route from run time routing table
=>	STAT PPP	Display PPP link status
=>	STAT HOST	Display current run time host table status

Table 4
LD 117: Maintenance PPP (cont'd.)

Prompts	Commands	Description
=>	STAT ROUTE	Display current run time routing table status
=>	SET MASK	Set ELNK subnet mask to configured value

Fault clearance

The three types of fault conditions that can occur during a PPP session are:

- transmission
- connection
- system related faults

Transmission Faults

Due to the characteristics of asynchronous communication, data transmitting over the serial interface can be corrupted at the receiving end. This type of error is detected by the receiver hardware as a CRC check sum. Should such a condition become a problem, disconnect the link and reconnect it at a lower baud rate.

Connection faults

A connection fault occurs when hardware failure takes place, or when the link carrier becomes lost. When a connection fault condition is detected, the faulty hardware must be replaced and the link carrier must be reestablished. The PPP link layer can still be connected, so you must either wait for the software to tear down the link after its timer expires, or issue the pppEnd command in PDT to force the link to shut down before attempting to reconnect the link.

System faults

A system fault is related to the system SDI operation state. All system SDI ports used for the PPP link must be configured in the system database and enabled after the sysload and INITs. When sysload or INIT occurs out of sequence, the SDI link disconnects and causes the PPP stack to close down. When such a condition occurs, re-establish the physical link and start the PPP link again.

Security

Security for establishing PPP links requires the same login name and password process imposed by the system. Once the PPP link is established, the application residing on the system can provide additional security if needed. Services provided by network operating systems,

such as Telnet and rlogin, can be provided by the host machine. System security access to Limited Access Password (LAPW) is supported in LD 117.

SSH and secure remote access

Secure Shell (SSH) provides a secure method to log on to a system remotely and perform system management operations. Using role definitions, specific users can be allowed to use SSH to connect to all parts of the system, or only to the parts specified by an administrator. This can include access to SL1 on the Call Server, support for the CPSID user name and ptyxx user names, access to the Call Server PDT shells, the Voice Gateway Media Card (VGMC) shell, IPL shell, and the Signaling Server OAM shell.

Unauthorized access to data

Some of the network services provided by the operating system can allow unauthorized access to system data. Table 5 "Network services available/access" (page 46) lists the services available.

Table 5
Network services available/access

Network Service	Type	Access Security	Comments
Telnet	Remote login	High	Host machine provides access security check
rlogin	Remote login	High	Host machine checks login name/password
FTP	Remote File Access	Low	Only accessible through PDT
NFS	Remote File Access	Medium	Only client protocol is supported
RSH	Remote File Access	Medium	Not supported

Possible data corruption

Most of the data being used for a PPP link is read from the configuration file when the process starts. The run-time data is stored in system memory and cannot be accessed by the user. In the case of a memory crash, the PPP process must be restarted to restore the run-time parameters.

System performance

The overall PPP link performance and system operational degradation depends on the amount of data exchanged between the system core and other applications. The amount of data includes the actual data being transferred, the protocol headers, and the re-transmission due to a CRC error. The actual data being transferred between the system core and applications is limited to the type of task running. The protocol overhead (such as PPP, IP, and TCP) is a fixed number of bytes for each data

frame. The only part that can be improved is the re-transmission rate. A good quality modem and line connection can reduce the re-transmission rate, and a smaller data frame size can improve performance.

Current system serial I/O generates an interrupt for every character it receives. With smaller data frame sizes, fewer interrupt services are required for each data frame and a better re-transmission rate results. This improves the PPP link performance and frees the CPU for other important tasks, such as call processing.

LAN access

The system Input/Output Processor cards are connected to the LAN. The system core is connected to its APs through the Application Module Link (AML) or a High-Speed link, allowing the LAN link to be managed and configured.

APs such as Meridian Mail (MM) and Integrated Call Center Manager (ICCM) have an Ethernet network interface. They can be connected to the system ELAN subnet.

Operating parameters

The system is accessed from the industry-standard ELAN network interface with the rate of transmission of 10 Mbits/second.

The use of ELAN network interface is restricted to Nortel-managed products.

Commands

The following table, Table 6 "Summary of commands" (page 47), provides a summary of LAN access commands.

Table 6
Summary of commands

Overlay	Commands
LD 117	Contains commands that you can use to configure and print the host names and IP addresses.
LD 137	Contains ENL, DIS, and STAT ELNK commands that you can use to enable, disable, and check the status of the Ethernet link.

Data included in datadump is available through LD 43.

Network address

Ethernet address

An Ethernet address is a 6-byte (48-bit) address, also called a MAC address. It is a unique physical address assigned to the Ethernet controller equipped in the I/O Processor (IOP). An example of a MAC address is: 00-08-74-4C-7F-1D.

On a redundant system, there are two IOPs; therefore, there are two Ethernet addresses. Although there are two physical Ethernet connections to the system core, there should be only one active connection for communication while the system is in the redundancy mode. Therefore, software configures both IOPs to use only one Ethernet address for communication over the link.

IP address

An IP address is a 4-byte (32-bit) address configured manually by the user. The IP address is also called the Internet address. Every IP address is associated with a host name. An example of an IP address is: 255.255.255.255.

On a redundant system, two IP addresses and host names must be specified: Primary and Secondary. Normally, the Primary IP Address (PIPA) is always used by the system. The Secondary IP Address (SIPA) can be used only when the system is operating in split mode (for a software or hardware upgrade).

This IP address and host name specification is provided by a file on the hard disk and can be referred to as the network address database file. For a single CPU configuration system, both IP addresses can be specified in this file, but only the Primary is used.

A default network database file is manufactured and shipped to the customer as part of the default database file sets. This database file contains the two default IP addresses and host names. Therefore, there is no need for a technician to configure the IP address at the customer's site in order to communicate with the system core. The technician can then change the default values to the new values by using LD 117.

The default network address database file is one of the system's Hardware Infrastructure (HI) database set. When the system performs a database backup, the database file is backed up to the floppy disk. When the customer performs a database restore, this file is also restored from floppy disk onto the hard disk.

Input/Output Processor configuration

Every Input/Output Processor (IOP) card is equipped with a Local Area Network Controller for Ethernet (LANCE) and is pre-configured with a unique MAC address.

In order for the system to communicate over the Ethernet link, it must be configured with both an IP address and a MAC address. System software handles the address resolution so that both the IP address and MAC address are configured correctly when the system starts, switches over, or is split.

Operating parameters

Administration of IP addresses and maintenance of the LANCE can be only done when the system task is active. Administration cannot be done from the OS/PDT shell level.

The IP address cannot be configured because the address is configured at the manufacturing site.

The same default IP addresses and host names are shipped to all customers' sites.

The system supports the existing Ethernet controller from Advanced Micro Devices (AMD) only.

To communicate with the inactive CPU side through Ethernet, the system must be in split mode.

This feature does not provide traffic report capability.

LD 117 is limited to one user at a time for the administration of IP addresses and host names.

Administration of IP addresses and maintenance of the LANCE is done through LD 137. LD 137 does not support maintenance telephone capability.

System components

On the system core's end of the LAN, an Ethernet connection is provided to connect the IOP's backplane from position 16F to the I/O panel. This cable is pre-installed at the factory and its code is NT7D90. The rate of transmission is 10 Mbits/second.

The customer must provide a 15-pin Attachment Unit Interface (AUI) cable to connect from the I/O panel to the Media Access Unit (MAU). The MAU is connected to the Ethernet Bus. The customer also needs to provide the MAU.

The compatible AUI types are:

- 10Base5 Type A
- 10Base2 Type B (cheapernet)
- 10BaseT (unshielded twisted pair)

Network management

Serial Line Interface Protocol support

The network management feature does not impact the current Serial Line Interface Protocol (SLIP) operation.

Point-to-Point Protocol support

For remote access to and from the system, PPP is supported. Refer to "Point-to-Point access" (page 37).

Physical link

Only Ethernet is supported. Other links such as Token Ring, Fiber Distributed Data Interface (FDDI), and Asynchronous Transfer Mode (ATM) are not supported.

Description

Default IP address and Host Name

The Primary and Secondary IP addresses and Host Names of the system core are set to default values by the manufacturer. As part of the system Default Database, the Primary and Secondary IP addresses and Host Names are installed on the system through the existing Installation tool.

The default IP addresses are in the B class, and the default host names are listed in Table 7 "Default IP address and Host Name" (page 50).

Table 7
Default IP address and Host Name

Field	Default Setting
Primary IP address	137.135.128.253
Primary Host Name	PRIMARY_ENET
Secondary IP address	137.135.128.254
Secondary Host Name	SECONDARY_ENET

Operation

Call Processor (CP) system state

Single CPU system For a single CPU configuration system, the Primary address and host name are used as the network address. The secondary address and host name are never used.

Redundant CPU system For a dual CPU configuration system, as long as the system is in redundant mode, the Primary address is used as the communication network address. The three operations that the core system must take into account are:

1. **CPU switchover:** When this happens, the system core software handles the network address resolution so that current connections over Ethernet work transparently on the new CPU side. This allows a

single Ethernet connection to the system. The switchover is activated by the following conditions:

— Software (graceful) switchover decided by system.

— Hardware (graceful) switchover decided by the system when power fails on the CPU. This occurs when a failure is detected by a watchdog-timer.

— Manual (forced) switchover by the SCPU command in LD 135.

— Hardware (forced) switchover. This occurs when the technician turns the switch on the CP card to the maintenance position.

2. **CPU split:** When this happens, the system core software handles the network address resolution by setting each CPU side as a different address so that both sides can communicate over the link, allowing dual connections to the system. The current active side remains connected using the Primary address. The "just-wake-up" side uses the Secondary address. The split is activated by the following conditions:

   — manual (forced) CPU-split by command ’SPLIT’ in LD 135.

   — hardware (forced) CPU-split by the technician, when the switches on the CP card side 0 and side 1 are both in the maintenance position.

   — boot-up (selected by a technician) system in split mode.

3. **CPU redundancy:** When the system is redundant, the system core software handles the network address resolution by setting the active CPU side so that it can communicate over the LAN. There is no communication with the inactive CPU side. A single Ethernet connection is used. System redundancy mode is activated by the following conditions:

   — manual (forced) redundancy by command ’SHDW’ in LD 135

   — hardware (forced) CPU redundancy by a technician, when the switches on CP card side 0 and side 1 are both in the normal position

   — boot-up (selected by a technician) system in redundancy mode

The table, Table 8 "System states and Ethernet connections" (page 52), summarizes the possible states of a redundant system and the state of the Ethernet connection being used

Table 8
System states and Ethernet connections

Switch set on CP side 0	Switch set on CP side 1	State of System	State of Ethernet Connection:
normal	normal	Redundant mode, either side can be active	Single connection to the active IOP
normal	maintenance	Side 0 is stand-by, side 1 is active	Single connection to IOP side 1
maintenance	normal	Side 0 is active, side 1 is stand-by	Single connection to IOP side 0
maintenance	maintenance	Split mode, either side can be active	Dual connection to both IOPs

Core I/O Processor card state

Because the LANCE is equipped on the IOP card, the state of the IOP has an effect on the LANCE. You can change the state of the IOP using the following commands in LD 137:

- Disable the active IOP using the command 'DIS IOP'. When you execute this command, the LANCE is disabled and becomes inaccessible.
- Enable the active IOP using the command 'ENL IOP'. When you execute this command, the LANCE is enabled and becomes accessible.
- Check the status of the active IOP using the command 'STAT IOP'. The status of LANCE is also checked, and the Disable or Enable state is printed.
- Check the status of both IOPs and Core Module Disk Units (CMDU) using the command 'STAT'. The status of both LANCEs (both CPU sides) are checked, and if the status of LANCE is disabled, an Out-Of-Service (OOS) message is printed to indicate the reason.

You can also enable or disable the IOP using the Enable/Disable switch on the card's faceplate:

- Disable the active IOP card by turning the switch to 'Dis' position. The LANCE is disabled.
- Enable the active IOP card by turning the switch to 'Enb' position. The LANCE is enabled.

The LANCE is also re-enabled if you remove and re-insert the IOP.

IOP power-up reset When you turn on the IOP card, a self-test on the subcomponents of the pack is initiated. For LANCE, the following tests are performed by the IOP's self-test manager:

- LANCE detection test. This consists of a routine that determines whether or not a given IOP pack is equipped with LANCE.
- LANCE's Private SRAM test. Read/Write memory test of this SRAM is performed.

During power-up, bus errors and timeouts are handled by the ROM-based Exception handler, which causes a HEX code to appear on the faceplate describing the problem.

IOP hex display message A hex code indication appears on the faceplate when LANCE fails the IOP Power-up self-test.

Abnormal operation

The three types of errors related to the Ethernet link are:

- Maintenance: to conform with the design of existing overlays, any maintenance error message related to LANCE will be composed of CIOD and an error code.
- Administration: any administration error will be in SCH format.
- Run-time error: format is composed of COM (Data Communication) and an error code.

Reset the LANCE when either of the following errors occur:

- LANCE memory response failure error
- Buffer error

If your attempt to reset the LANCE fails, the system attempts to switch CPUs.

Service change

LD 117

Administer the host names and IP address using LD 117. Table 9 "Ethernet configuration" (page 54) illustrates how to change the host name and IP address for the Primary and Secondary CPU side. Refer to "Direct Gateway Access" (page 68).

Ethernet configuration Table 9 "Ethernet configuration" (page 54) shows the prompt sequence and responses for configuring the Ethernet link in LD 117.

Table 9
Ethernet configuration

Prompt	Response	Description
>LD 117	OAM000	User types this command to load LD 117.
=>CHG ELNK ACTIVE PRIME_HOST	INET Database updated	User enters the change ELNK followed by active and the host name to change the IP and host name for Primary. The host name must exist in the host table.
=> CHG ELNK INACTIVE SEC_HOST	INET database updated	User enters the change ELNK followed by inactive and the host name to change the IP and host name for Secondary. The host name must exist in the host table.
=>	...	

After configuring the address, you must restart the system.

Supported Host Name length The maximum length for the Host Name is 16 characters. The minimum length is 1 character. The first character of the host name must not be a digit.

Supported Host Name characters The host name you enter must conform to the following:

- A valid host name consists of a text string that can include the alphabetic characters ’a’ to ’z’, the digits ’0’ to ’9’, and the underscore (_).
- The period (.) is not permitted in the host name because it is reserved for use as a delimiter between domain names.
- No space or tab characters are permitted.
- The first character of the Host Name must be an alphabetic character (a to z).
- There is no distinction between upper case and lower case.

The system prints an error message if you enter a host name that does not meet the guidelines listed above.

Print ethernet addresses To display the primary and secondary IP addresses and host names from LD 117, use the command shown in Table 10 "Display primary and secondary IP addresses and host names" (page 55).

Table 10
Display primary and secondary IP addresses and host names

Prompt	Response	Description
=> PRT ELNK		Type this command to display the Ethernet configuration.
ACTIVE ETHERNET: "PRIMARY_ENET""137.135.128.253" INACTIVE ETHERNET: "SECONDARY_ENET" "137.135.23.50"	OK	The primary address, secondary address, and host names and addresses are displayed.

Ethernet reset To reset the Primary and Secondary IP addresses to default values, use the commands in LD 117, as shown in Table 11 "Ethernet reset" (page 55)).

Table 11
Ethernet reset

Prompt/Command	Response	Description
=> RST ELNK ACTIVE	INET Database updated	Type this command to reset the Primary IP address to the default value
RST ELNK INACTIVE	INET Database updated	Type this command to reset the Secondary IP address to the default value.

Traffic measurements and CDR outputs There are no Ethernet traffic or CDR outputs generated by the system.

Fault clearance procedure

Reset the Ethernet link by using LD 137 to disable and enable the Ethernet link. Restarting the system has the same effect. Resetting the link clears all error flags on the LANCE and re-initializes it.

When a run-time problem is encountered for the Ethernet link, an error message is displayed.

Security

All LD 117 users are allowed to administer the IP address.

The Multi-user feature prevents more than one user from loading LD 117 at the same time.

Hardware requirements

To have Ethernet operate in the ELAN subnet, the following is required:

- System is equipped with IOP, the LANCE AM7990 and AM7992B Serial Interface Adapter (SIA). This configuration is pre-assembled at the factory.
- Cable connects IOPs backplane to I/O panel. This is pre-configured at the factory.
- AUI cable connects I/O panel to MAU.
- MAU (transceiver)
- Ethernet backbone

Communication devices

To communicate with the system through a system terminal, a Video Display Terminal (VDT) or a Teletypewriter (TTY) must be connected directly to the system I/O port, or remotely through an asynchronous modem connected to the system I/O port.

Device characteristics for the non-MSDL I/O port are shown in the table: Table 12 "Device characteristics for the non-MDSL I/O port" (page 56).

Table 12
Device characteristics for the non-MDSL I/O port

Characteristic	Acceptable Value
Interface	RS-232-C
Code	ASCII
Speed	110, 150, 300, 1200, 2400, 4800, 9600 baud; also 14200 or 38400 baud if MSDL is used
Loop current	20 mA
Terminal emulation	VT220

Device characteristics for an MDSL I/O port are shown in the table: Table 13 "Device characteristics for an MDSL I/O port" (page 56).

Table 13
Device characteristics for an MDSL I/O port

Characteristic	Acceptable Value
Interface	RS-232-C or RS-422
Speed	300, 1200, 2400, 4800, 9600, 19200, 38400 autobauding
Flow control	Xon/Xoff supported
Terminal emulation	VT220, 8-bit with line mode editing or STA

Supported devices include the following:

- input/output:
  - RS-232-C compatible Video Display Terminal (VDT) (also referred to as a system terminal)
  - PC with a serial port
  - Attendant Console
  - RS-232-C compatible Teletypewriter (TTY)
  - VT100 TTY type interface
  - VT220 with 7-bit or 8-bit mode with access to subsystems through STA using MDSL
- input only:
  - maintenance telephone used to provide limited access to the following Overlays: LD 30, 32, 33, 34, 35, 36, 37, 38, 41, 42, 43, 45, 46, 60, 61, and 62
- output only:
  - RS-232-C compatible printer (PRT)

Log on and log off

Because the system supports multiple users, it provides security features to help ensure system integrity. One of these features requires that you complete a login sequence to begin an online session. For more information about security features, see “Security” (page 72).

For detailed procedures on logging into UCM and accessing managed elements, see *Unified Communications Management - Fundamentals* (NN43001-116).

To log on as administrator, enter the logon command (LOGI) followed by a valid user name and password. You can change the password using LD 17.

Use Procedure 1 “Using a VDT to log in, load a program, and log out” (page 58) to log in to the system from a VDT. Use Procedure 2 “Using a maintenance telephone to log in, load a program, and log out” (page 60) to log oin to the system from a maintenance telephone.

Procedure 1
Using a VDT to log in, load a program, and log out

Step	Action

1 Press <cr>.

If the response is:	Then:
A period (.)	You can log in. Go to Step 2.
OVL111 nn IDLE	You can log in. Go to Step 2.
OVL111 nn BKGD	You can log in. Go to Step 2.
OVL111 nn TTY x	You cannot log in now. You must wait until another user logs off and then retry.
OVL111 nn SL1	You cannot log in now. You must wait until another user logs off and then retry.
OVL000 >	You are already logged in. Go to Step 4.

2 Type the following command to log in to the system:

```
LOGI <cr>
```

–or–

```
LOGI <user name> <cr>
```

- If the response is PASS?, go to step 3.
- If the response is an error message, refer to *Software Input/Output: System Messages* (NN43001-712).

3 Type the Level 1 or Level 2 password followed by <cr>.

- If the response is **>**, go to 4.
- If the response is an error message, refer to *Software Input/Output: System Messages* (NN43001-712).

4 Type a command in the following format to load a program:

```
LD xx <cr>
```

–or–

```
LD xxx <cr>
```

5 Perform the necessary tasks.

6 Type the following to end the current program:

```
END <cr>
```

–or–

```
**** <cr>
```

7 To load another program, go to 4.

To end the session and log out, type the following:

```
LOGO <cr>
```

--End--

Use a maintenance telephone for one of the following reasons:

- The TTY port is not available or not operational.
- Access to the maintenance telephone is more convenient than access to the TTY port.
- To generate test tones.

When using a maintenance telephone, use telephone keys that correspond to letters and numbers on a system terminal.

For example, on a system terminal, enter:

```
LD 42 <cr>
```

On a maintenance telephone, enter:

```
53#42##
```

Table 14 "Keyboard-to-telephone key mapping" (page 59) maps the keys on a system terminal keyboard to the telephone keys on a maintenance telephone.

Table 14
Keyboard-to-telephone key mapping

Keyboard				Telephone
			1	1
A	B	C	2	2
D	E	F	3	3
G	H	I	4	4
J	K	L	5	5
M	N	O	6	6
P	R	S	7	7
T	U	V	8	8
W	X	Y	9	9

Note: There is no Q or Z on a telephone.

Table 14
Keyboard-to-telephone key mapping (cont'd.)

Keyboard				Telephone
			0	0
		Space or #		#
		Return		##
Note: There is no Q or Z on a telephone.				

Procedure 2
Using a maintenance telephone to log in, load a program, and log out

Step	Action
1	Press the prime DN key.
2	Type the following to place the telephone in maintenance mode: **xxxx91** where **xxxx** is the customer's Special Prefix (SPRE) number. The SPRE is typically **1**, in which case, type **191**. The Customer Data Block defines the SPRE. Print it by using LD 21. or Enter the appropriate Flexible Feature Code (FFC). The FFC is usually 30. See *Features and Services (NN43001-106)*.
3	Key the following to check for a busy tone: **##** If there is no busy tone, go to step 4. If there is a busy tone, another program is active. The two choices are: • try again later • end the active program and gain access to the system by typing: ********
4	Type a command in the following format to load a program: **53# xx ##** where **xx** is the number of the program.
5	Perform the necessary tasks.

6 Type the following to end the current program and return the telephone to processing mode: enter: ****

--End--

Background routines are then loaded automatically.

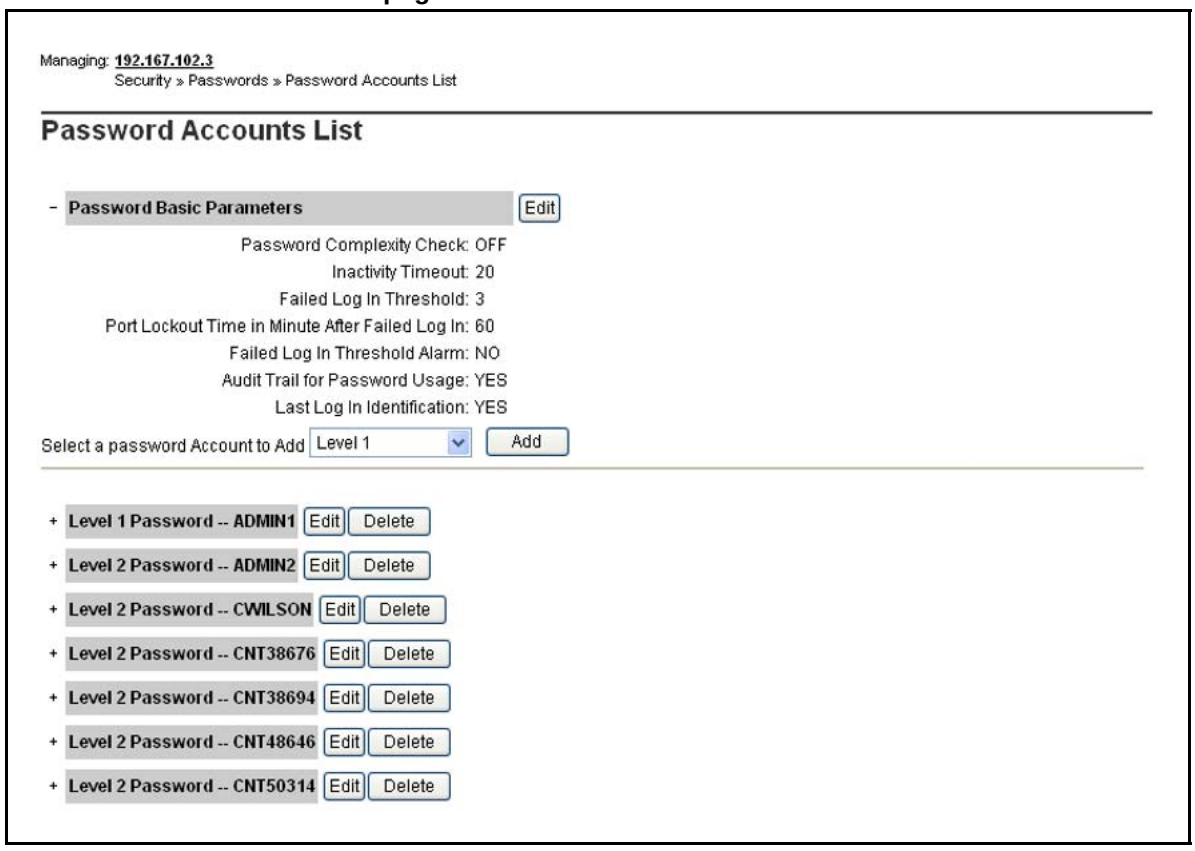
Element Manager Password function

The Element Manager Password function performs the same tasks as the PWD-related CLI commands traditionally configured in LD 17.

Note: The System Passwords link is applicable only to systems which have the radius authentication turned off.

To access the password modification functions, click the **Passwords > System Passwords** link in the **Security** branch of the Element Manager navigator. The **Password Accounts List** web page opens, as shown in Figure 9 "Password Accounts List web page" (page 61).

Figure 9
Password Accounts List web page



Force Password Change in Element Manager

Only a Level2 user can access the Password Basic Parameters. When the Force Password Change (FPC) feature when is turned On, PWD and PDT users logging in with default passwords must change their passwords before continuing.

Procedure 3
Changing password basic parameters

Step	Action
1	From the **Password Accounts List** web page, click the **Edit** button next to Password Basic Parameters. The **Password Basic Parameters** web page opens. See Figure 10 "Password Basic Parameters web page" (page 63).
2	Select the **Force Password Change (FPC)** checkbox.
3	Enter the **Level 2 Password (LVL_2PWD)**.
	--End--

During the next login, the user is prompted to change the system passwords, as shown in Figure 11 "System password change" (page 63).

Figure 10
Password Basic Parameters web page

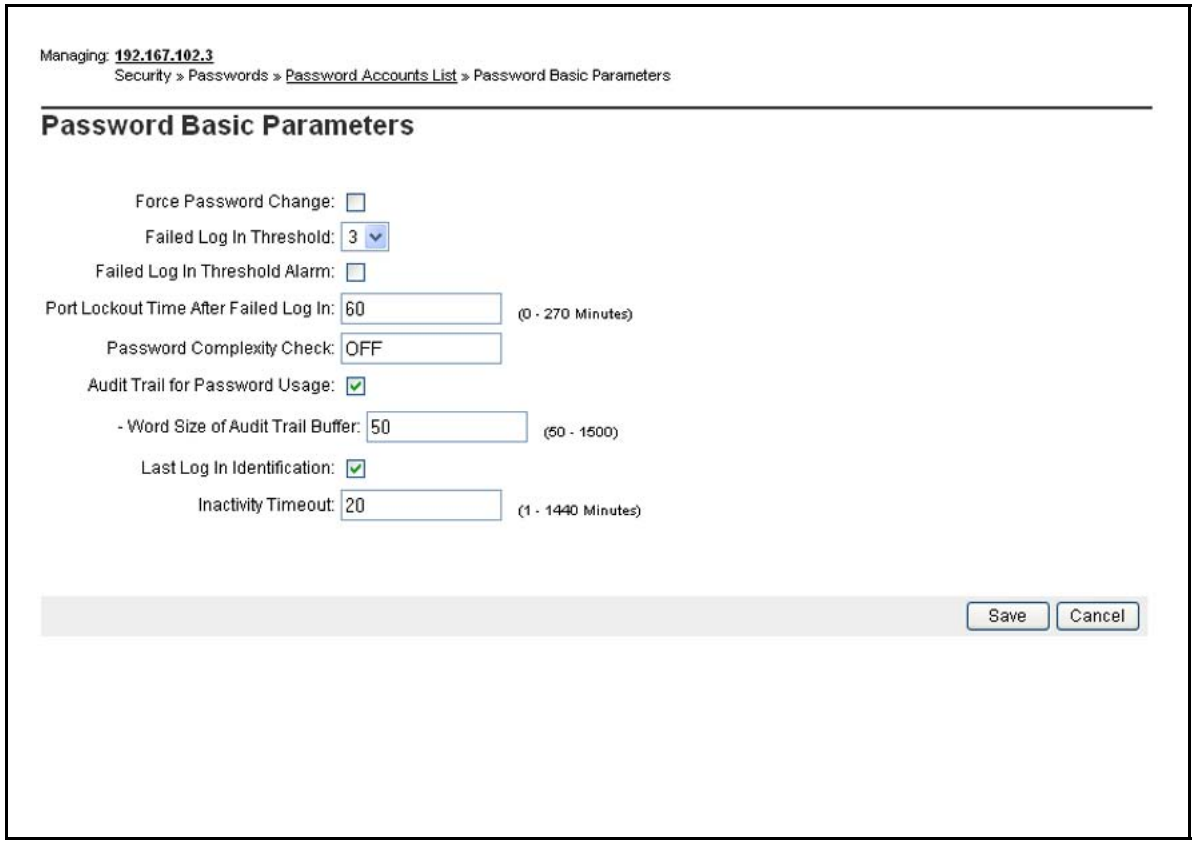
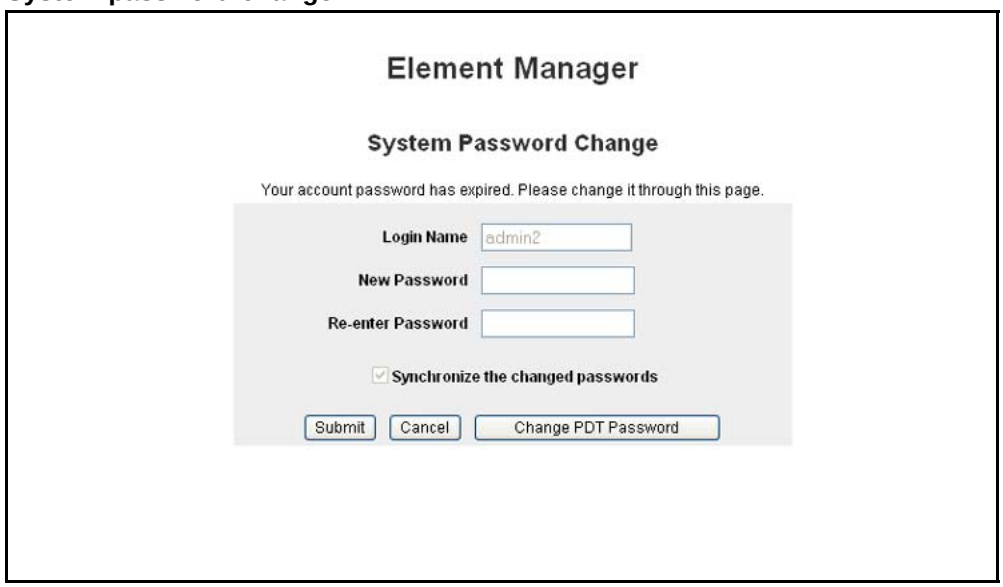


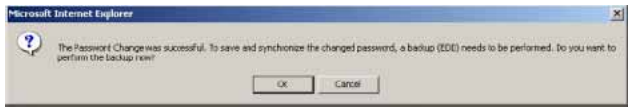
Figure 11
System password change



Synchronize changed Passwords

This option is selected by default and will perform a datadump in the Call Server after the passwords are changed successfully. The datadump is required to synchronize the password across the servers linked to the Call Server. See Figure 12 "Synchronize change passwords" (page 64).

Figure 12
Synchronize change passwords



Administrative and maintenance programs

Administrative and maintenance programs reside on disk and are loaded into the RAM overlay area when they are needed. To enhance performance, certain programs are loaded immediately into cache memory or system RAM. Other programs are loaded in response to an instruction from the CPU or a command from a system terminal, maintenance telephone, or Attendant Console. The programs are often referred to as overlays because of how they are loaded.

Maintenance programs

Maintenance programs perform hardware and software diagnostics. They also enable, disable, and check hardware status.

- Background

  When users are not running maintenance overlays, special maintenance programs run continuously in the background to monitor system performance. These programs detect system discrepancies before they begin to affect service. When there is sufficient CPU capacity, background routines also execute a set of overlays to ensure the integrity of the system.

- Midnight or Daily Routines

  In addition, a set of maintenance programs runs automatically once a day, usually at midnight. These are called daily or midnight routines. Results of selected tests run by these routines may appear on the TTY. The system prints a banner page to indicate the beginning and ending of each daily routine. The content of the banner page is as follows:

  DROLXXX <Overlay Mnemonic> <LD xx> <BEGIN, END> <Time stamp>

  The following is an example of the banner pages for a daily routine:

  DROL000 NWS LD 30 BEGIN 00:35 23/1/92

.

.

.

DROL001 NWS LD 30 END 00:42 23/1/92

- Manually Loaded

  Many maintenance programs use a command/action/response format. Enter a command, and the system performs the requested action and responds with the result. The table Table 15 "Maintenance program commands" (page 65) shows an example of a command recognized by several different maintenance programs.

Refer to *Software Input/Output: Administration (NN43001-611)* for the complete list of maintenance programs, as well as their prompt/response sequences.

Table 15
Maintenance program commands

Overlay	Command	Explanation
02	STAD dd mmm yyyy hh mm ss	Configure telephone time and date.
30	STAT	Check the status of network loops.
135	STAT CNI	Check the status of the CNI port.

When you load a maintenance program, it replaces any currently running background program with the exception of LD 44. Administrative routines (such as LD 10 and LD 11) do not abort background routines.

Administration programs

Administration programs implement and modify system features and reflect changes in system configuration. For example, a system administrator uses administration programs to make changes to directory numbers, telephones, trunks, and features.

Once loaded, administration programs use a step-by-step prompt/response format. The program issues a prompt for input, and the administrator enters the appropriate response through the keyboard, followed by the **Return** key. The **Return** key signals the end of each response. Table 16 "Using an administration program" (page 66) shows an example of how to use an administration program.

Table 16
Using an administration program

Prompt	Response	Description
REQ	CHG	The program requests input; the response indicates the need to change some data.
TYPE	CFN	The program asks what type of data to change; the response indicates that the data is in the Configuration Record.
PARM	YES	The program asks if the change is to a system parameter; the response confirms that it is a change to a system parameter.
- ALRM	YES	The program asks whether to enable the minor alarm on attendant consoles; the response confirms that the alarm is to be enabled.
REQ	****	The program prompts for more input; the response ends the program.

If the response is valid, the system program issues the next prompt. If the response is invalid, the program issues a message using the format SCHxxxx, where SCH stands for Service Change, and xxxx is the specific message identifier. See *Software Input/Output: Administration (NN43001-611)* for an explanation of each SCH message.

Program loading

After logging in on a system terminal, type the following to load a program:

```
LD xx <cr> {for TTY}
```

–or–

```
LD xxx <cr> {for Maintenance Set}
```

Overlay characteristics

This section describes some of the characteristics of the administration programs.

Data groups and gate opener prompts An individual prompt can be accessed using a special gate opener prompt to its data group. For example, PWD is the LD 17 gate opener to prompts related to passwords. See sample gate opener prompts in Table 17 "Sample gate opener prompts in LD 17" (page 67).

Gate opener prompts improve administration productivity by eliminating the need to step through numerous prompts to access and modify a specific value.

By entering a gate opener mnemonic in response to the TYPE prompt in LD 17, the user gains access to its data group. See *Software Input/Output: Administration (NN43001-611)* for further detail.

Table 17
Sample gate opener prompts in LD 17

Mnemonic	Description
ADAN	All I/O devices, including D-channels
ATRN	Meridian Modular Telephone transmission parameters
CEQU	Common equipment data
OVLY	Overlay Area options
PARM	System parameters
PWD	System Password and Limited Access to Overlays Password
VAS	Value Added Server data

When exiting a gateway, the updates for the data group are written to Protected Data Store. Canceling out of the program does NOT cancel the updates.

The LD 22 Print Routines for the Configuration Record support printing individual data groups as well as the entire data block. The print sequence is identical to the data entry prompt sequence in LD 17.

Table 18 "Sample gateway prompts in LD 22" (page 67) lists some data group mnemonics entered at the TYPE prompt in LD 22.

Table 18
Sample gateway prompts in LD 22

Prompt	Description
CFN	Print complete Configuration Record (excluding password data) (See PWD below.)
ADAN DCH <x>	Print one or all D-channel (and associated backup D-channel) information
ADAN HST	Print History File
ADAN FDK	Print floppy disk configuration
ADAN TTY <x> ADAN PRT <x>	Print information for one or all system terminals
ADAN AML <x>	Print one or all Application Module Links
ADAN	Print all I/O device information
PWD	Print System Password and Limited Access to Overlay Password (requires that the user be PWD2)
PARM	Print system parameters
CEQU	Print common equipment data
OVLY	Print Overlay Area options
VAS	Print Value Added Server data
ATRN	Print Meridian Modular Telephone transmission parameters

Enhanced Input Processing Enhanced Input Processing accepts up to 80 characters of input collection for selected prompts before processing. Line-oriented parsing does not pass the input characters to the overlay until either the 80-character limit is reached or a **Return** key is detected. In addition, a user can request a list of valid responses to a specific prompt by entering:

```
?<cr>
```

Prompts supporting this function have a colon appended as a suffix:

REQ:

The user can also enter abbreviated responses. The overlay responds with the nearest match to the expected response. The user can change this response if it is incorrect.

Direct Gateway Access

Operating parameters Direct Gateway Access is available by entering its mnemonic at the TYPE prompt. The user can still enter CDB in response to TYPE and receive a YES/NO gate opener prompt for each of the 25 gateways.

For more detailed information, see *Software Input/Output: Administration (NN43001-611)*.

The user can enter DEFAULT at TYPE to create a new data block. This enables the user to create a default CDB without going through many prompts.

Overlay Supervisor

The Overlay Area is an area of program store (approximately 20K words in size) reserved for Operations, Administration, and Maintenance (OA&M) programs. These programs, identified by a two- or three-digit number, reside on the system mass storage (hard disk, floppy disk, or tape). The Overlay Supervisor handles the loading and execution of the overlays, accepting requests from a TTY, predefined BCS pad, or the system itself.

The two types of input that affect the Overlay Supervisor are loop input (peripheral signaling) from maintenance busy equipment and teletype input.

The Overlay Supervisor performs the following functions:

- Controls all devices that are executing overlays.
- Monitors TTY activity and disables any TTYs that appear to be faulty.

- Translates TTY input and maintenance telephone input to appear identical to the Operator and Task processes.
- Controls session if Multi-User Login is turned on.

The following task is required: The Operator process handles Overlay Supervisor commands such as LOGI. The Task process monitors executing overlays.

- Routes input to the appropriate destination, either the Login process, Operator process or the Task process.

Timeout

If a user is logged in to a session, each keystroke on the terminal resets the timeout back to 30 minutes. If long reports are being output by an overlay the overlay resets the timeout back to 30 minutes after each timeslice. Only after the terminal is idle for 30 minutes, is the user logged off.

Cache memory

With Overlay Cache Memory implemented, when an LD xx command is received, the system checks cache memory to determine if it contains the requested overlay. If so, the system rapidly copies the overlay data portion to a regular overlay area, and executes the overlay from the cache memory area.

If the specified overlay is not in cache memory, the system loads it from disk into a regular overlay area. At the same time, it is also loaded into one of the 32 cache memory areas.

The technician can ensure that an overlay is loaded from disk by using the LD xx D command. If the overlay also resides in cache memory, the newly loaded copy overwrites the existing copy. The message "Please wait – loading from disk" and/or the blinking disk LEDs confirm that the overlay is being loaded from disk.

Linked programs

To further simplify program access, a mechanism links several overlays and permits the user to move between them. This mechanism accepts commands entered in one program and directs them to the appropriate linked program, eliminating the need to explicitly exit one program and invoke another.

Table 19 "Examples of Linked overlays" (page 70) shows some examples of the linked programs.

Table 19
Examples of Linked overlays

Overlay	Linked overlay
LD 10/11	LD 20 with PRT, LUC, LUU, or LTN command; return to LD 10/11 with NEW or CHG command.
LD 10/11	LD 32 with ENLL or DISL command; return to LD 10/11 with NEW or CHG command.
LD 20	LD 10/11 with NEW or CHG command; LD 32 with any valid LD 32 command.

System Message Lookup Utility

The System Message Lookup Utility supports online lookups of system alarm messages. The utility accepts system alarm mnemonics and provides a descriptive explanation of the event. It supports Lookup Last Error and Lookup Any System Message. For more information, see “Fault Management” (page 86).

Multi-user considerations

Multi-User Login allows up to five users, and a background or midnight routine, to execute overlays concurrently. Special software prevents conflicting overlays from executing at the same time. Multiple copies of certain overlays can execute at the same time. These include administrative LD 10 and LD 11. Also, multiple copies of print LD 20, LD 21, and LD 22 can also execute concurrently.

Multi-User Login also provides directed I/O: input and output during a user’s session appears only on that user’s TTY.

For more information, refer to “Multi-User Login” (page 136).

Using programs

Special characters

The characters shown in Table 20 "Special characters and their meaning" (page 70) have a special meaning to the software.

Table 20
Special characters and their meaning

Character	Meaning
**	Repeat current prompt.
*	Return to REQ prompt.
****	End the current program.

Table 20
Special characters and their meaning (cont'd.)

Character	Meaning
Prompt: !	Help implemented, use question mark "?" to list valid responses. From within an executing overlay, invoke and execute the system command that immediately follows the exclamation point: !WHO See "Multi-User Login" (page 136) for a list of these system commands.

Line Mode Editing

For MSDL/SDI with Line Mode Editing (LME), the user can enter and review an entire line before transmitting it to the system. This function is only supported for VT220-type terminals running EM200 emulation mode.

Printing

Table 21 "Print programs and data" (page 71) lists the print programs and the type of data they can print.

Table 21
Print programs and data

LD	Type of Data	LD	Type of Data
20	Data Access Card Dial Intercom Group Directory Numbers Feature Group D Hot Line list Hunting pattern Multifrequency receivers Multifrequency versatile units Pretranslation data Speed Call lists Templates Terminal Number blocks Unused cards Unused units	22	Audit trail for Limited Access to Overlays Configuration Record Code inventory for Large System Directory Numbers History File IMS message attendant and software limits Issue and Release identifiers Equipped package list Passwords Peripherals software versions Read Only Memory (ROM) System loop limit Tape ID

Table 21
Print programs and data (cont'd.)

LD	Type of Data	LD	Type of Data
21	ATM routes ATM schedules CAS key Code Restriction data Customer Data Block Route data Set relocation data Trunk members	81	List or count telephones with selected features Date of last service change
		82	Telephone hunt patterns Multiple Appearance groups

For information on using gateways, see "System messages" (page 87)

For information on messages that may appear during program execution, see "System messages" (page 87).

Security

The system provides mechanisms to limit access to features and functions, and provides audit trails of user sessions. Extensive system-wide security features help detect and prevent possible unauthorized access.

All transfers between CS 1000 devices that are not performed manually must be done through a secure transfer. This provides security, and enables communications between the Call Server, Signaling Server and Voice Gateway Media Card.

For a comprehensive treatment of security topics, refer to *Access Control Management (NN43001-602)* and *Security Management (NN43001-604)*.

Media Security features encrypt transmissions between IP Phones, and IP Phones display a status icon to indicate when this feature is in operation.

The Default Password Change feature enhances security of the system (including the Call Server, Signaling Server, and Voice Gateway Media Card) by forcing users to change their system passwords.

For added security on remote connections, consider the following options:

- Use a dial-back modem with pre-assigned telephone numbers. The configuration of the modem and the dial-back feature depends on the make and model of the modem.
- Dial into a Remote Access Server and authenticate your login on the network before using Telnet to access the component.
- Dial into the modem on a workstation, and then use a remote control client such as PCAnywhere or Timbuktu to connect to the component

using Telnet. However, remote control clients can compromise security precautions.

Refer to “Local and remote access” (page 33) for more information on connectivity.

To help control unauthorized access, Nortel recommends the following:

- Store equipment in a physically secure area.
- Use perimeter security (such as router-based filtering or firewalls) to secure the ELAN subnet.
- Secure remote access through Virtual Private Networks.
- Institute a password management policy.
- Carry out security audits periodically.

Secure File Transfer Protocol

Secure Shell (SSH) Secure File Transfer Protocol (SFTP) is installed and enabled on Communication Server 1000 systems by default. This secure protocol replaces regular File Transfer Protocol (FTP) and other insecure data transfer protocols for several Communication Server 1000 applications.

SFTP allows data to be securely transferred between an SFTP client and server over an encrypted and authenticated secure channel. In addition, SFTP allows a client and a server to authenticate each other by using a password. Devices obtain authentication and access control permissions for CLI access from the Unified Communications Management Primary Security Server. Remote Authentication Dial In User Service (RADIUS) parameters are sent from the Unified Communications Management Primary Security Server to the Call Server using SSH protocol. SFTP uses port 22, which is the same port used by SSH.

The authentication process for internal transfers uses the UCM security token as part of the authorization process. All elements using SFTP for internal transfers must have the same security token as distributed and synchronized by the UCM Primary Security Server.

Not all Communication Server 1000 applications are compatible with SFTP. To provide backward compatibility for those features that are not compatible with SFTP, conventional FTP is still used for file transfer sessions between Release 7.0 systems and systems with previous versions. For systems and applications that are not compatible with SFTP, IPsec protocols are used for security.

The following characteristics apply to SFTP:

- The public key of a SFTP server is always trusted by SFTP clients, so there is no requirement for verification.
- ISSS security for specific elements can be disabled using the UCM Primary Security Server. When disabled, all communications from the specified IP address of the element are sent without IPsec to protect the messaging traffic to the other elements of the Communication Server 1000 system. Manual targets with ISSS disabled must be configured without IPsec; communications between other elements is not affected.
- A user name and password is used by a SFTP server to authenticate a SFTP client (public key-based authentication is not supported for authenticating a SFTP client). For internal automated transfers, the UCM security token is used to construct the password.
- TFTP for transferring tone and cadence files is not changed.
- Not all FTP applications use SFTP; some continue to use standard FTP.
- Interactive users of SFTP have restricted directory access.

For more information about Secure File Transfer Protocol, refer to *Security Management Fundamentals* NN43001-604.

Unified Communications Management Security

The Unified Communications Management (UCM) security framework enables element and service management applications to access a common application security infrastructure.

UCM manages secure access to Web applications and provides security for Web interfaces and Web utilities.

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

UCM provides access to various security features that enable system administrators to configure user and security rights within the application server.

UCM allows system administrators to create new roles and assign default built-in roles to users within UCM. Permissions for the role can be mapped for each user. Users see only what they are authorized to see based on their assigned roles and permissions.

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

You access Element Manager, Network Routing Service Manager, and Subscriber Manager, through UCM which provides the logon security.

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

Command Line Interface

When accessing the system from a remote location, the login security consists of a username and password combination, as configured with the system. These system logins come with defaults for the Limited Access Password (LAPW), and the Problem Determination Tool (PDT) Level 1 password and Level 2 password. These default PDT passwords must be changed. For more information, refer to *Access Control Management (NN43001-602)*.

Passwords

Passwords stored on the system are encrypted.

Administration passwords

System software provides two types of passwords that enable access to database configuration and maintenance programs:

- **Level 1 passwords (PWD1 or admin1)**: Use these passwords to gain general access to the system to perform administrative and maintenance tasks.
- **Level 2 passwords (PWD2 or admin2)**: Use these passwords to gain restricted access to the System Configuration Record to change passwords and perform other tasks related to the system.

You must be logged in with PWD2 to enter or change passwords in LD 17 PWD. The LNAME_OPTION in LD 17, which defaults to YES, indicates that login names are required. You can associate a user name with PWD1, PWD2, and any of 100 LAPWs. The user name can be up to 11 alphanumeric characters.

Good security practices include changing all passwords regularly. Valid passwords must:

- contain 6 to 16 characters
- never be duplicated (Level 1 and Level 2 passwords must not match)
- consist of digits 0 through 9 and characters A through Z (case-sensitive)

System components (such as Media Gateways, Signaling Servers, and Voice Gateway Media Cards) synchronize their login names and passwords to the Call Server's PWD1 if the Call Server is available. If not, they use their default login names and passwords.

Each component of the system also has its own password to access the operating system or the CLI of the component:

- Logging in to the Call Server or Media Gateway Overlays requires that the administrator enter the login command (LOGI) followed by a valid Level 1, Level 2, or LAPW password. See "Limited Access Passwords" (page 76).
- The Signaling Server uses the Level 1 password from the Call Server while a connection to the Call Server exists. The default CLI username on the Signaling Server is **admin**. See *Signaling Server IP Line Applications Fundamentals* (NN43001-125).
- When you log in to Element Manager, you are actually logging in to the Call Server. You receive the same permissions configured to your user ID on the Call Server.
- The NRS Manager requires a user ID and password to access the NRS. There are two levels of access: administrator access level and monitor access level. For more information, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*.
- For passwords on IP Phones (Station Control Password, IP Phone Installer Password, Temporary IP Phone Installer Password, Telephone Relocation password, Set Removal Password, or Set Relocation Security Code (SRCD), see *Branch Office Installation and Commissioning (NN43001-314)* and *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Limited Access Passwords

You can use Limited Access Passwords (LAPW) to restrict user access to overlay features, specific programs, and data. Use LD 17 on the Call Server to define up to 100 login passwords in the configuration record, each with its own set of access restrictions. For more information, refer to "Limited Access to Overlays" (page 113).

In Element Manager, a user can create LAPWs, and users with Level 2 access can change Level 1 and Level 2 logins and passwords. Refer to *Element Manager System Reference - Administration (NN43001-632)*.

PDT password

For the Call Server and Media Gateway, the PDT shell (which is an expert-level tool) is password-protected. For more information, refer to *Access Control Management (NN43001-602)*.

Secure Data Password

This password limits the service change of authorization codes in LD 88 on the Call Server.

History file

Call Server

The System History File provides a complete audit trail of all user sessions, including the following data:

- TTY number and (optionally) user name
- login and logout times
- periodic time stamps
- a list of overlays accessed
- session duration

In addition, the search facilities provided through the **VHST** command facilitate locating relevant messages in a large file.

The Multi-User Login feature enables you to direct TTY-session information to separate TTY log files. This is particularly useful to segregate system error messages from routine information messages. In addition, Multi-User Login enables you to track sessions on a TTY where unusual login activities have occurred.

Unified Communications Management Logon

Users launching Unified Communications Management (UCM) for the first time must change the default password.

Users can log on to UCM using various options such as high availability mode, Single Sign On (SSO), webauth servelet, and external authentication.

For detailed procedures on how to log on to UCM, see *Unified Communications Management Common Services - Fundamentals* (NN43001-116).

Software management

Contents

This section contains information on the following topics:

Introduction

The following describes the available tools supporting management tasks on CS 1000 and Meridian 1systems.

Configuration of data blocks and components

The following sections are a reference for the different configuration activities you can perform on components of the CS 1000and Meridian 1systems.

Command Line Interface

The CLI exists on the following platforms in the following formats for management and configuration capabilities:

- **Call Server and Media Gateways:** Administration and maintenance overlays, Problem Determination Tool (PDT, a debug tool which includes routine maintenance such as applying patches), and VxWorks command lines
- **Signaling Server:** OAM, PDT, and VxWorks command lines
- **Voice Gateway Media Cards:** IPL and VxWorks command lines

Call Server

Table 22 "Configuration of Call Server data blocks" (page 80) presents the configuration tasks and the user interfaces that are available for these tasks.

Table 22
Configuration of Call Server data blocks

Datablock	Overlay	Element Manager
Traffic	2	Yes Tools > Logs and Reports > Operational Measurements
Time and Date	2	Yes Tools > Date and Time
Analog telephones	10	Yes
IP and Digital telephones	11	Yes
Attendant Consoles	12	No
Digitone receivers, tone detection, multifrequency sender and receiver	13	Yes System > Core Equipment > Tone Senders and Detectors

Table 22
Configuration of Call Server data blocks (cont'd.)

Datablock	Overlay	Element Manager
Trunks	14	Yes Routes and Trunks > Routes and Trunks > Trunk Property Config
Customers AML ANI ATT AWU CAS CSS CDR FCR FFC FTR HSR ICP IMS INT LDN MPO NET NIT OAS PPM PWD RDR ROA TIM TST	15	Partial Customers > Customer Property Config
Route	16	Yes Routes and Trunks > Routes and Trunks > Route Property Config
Automatic Trunk Maintenance	16	No

Table 22
Configuration of Call Server data blocks (cont'd.)

Datablock	Overlay	Element Manager
Configuration Record 1 -ADAN -ATRN -CEQU -OVLY -PARM -PWD -VAS -ROLR/TOLR / APLR -HRLR / HTLR	17	Partial ***Note:*** The following are supported: ADAN Routes and Trunks> D-Channels > D-Channels Property Config CEQU System > Core Equipment > Loops (Common Equipment) PARM System > Interfaces > Property Management System PWD Security > Passwords > System Passwords VAS System > Interfaces > Value Added Server
Speed Call Group Call Pretranslation Special Service 16-Button DTMF Hotline	18	No
Code Restriction	19	No
Automatic Call Distribution Management Reports Message Center	23	No
Direct Inward System Access	24	No
E911	24	Yes System > Emergency Services

Table 22
Configuration of Call Server data blocks (cont'd.)

Datablock	Overlay	Element Manager
Group Do Not Disturb	26	No
ISDN Basic Rate Interface (BRI)	27	No
Route Selection for Automatic Number Identification	28	No
Memory Management	29	No
New Flexible Code Restriction	49	Yes Dialing and Numbering Plans > Flexible Code Restriction
Incoming Digit Conversion	49	Yes Dialing and Numbering Plans > Incoming Digit Conversion
Call Park and Modular Telephone Relocation	50	No
2.0 Mb/x Remote Peripheral Equipment	52	No
Flexible Tones and Cadences	56	No
Flexible Features Codes	57	No
Radio Paging	58	No
Digital Trunk Interface	73	Yes Routes and Trunks > Digital Trunk Interface
Digital Private Network Signaling System Link	74	No
Virtual Network Service	79	No
Set Designation Entry (ODAS)	84, 85	No
Electronic Switched Network 1	86	Yes Dialing and Numbering Plans > Electronic Switched Network
Electronic Switched Network 2	87	Yes Dialing and Numbering Plans > Electronic Switched Network
Authorization Code	88	No

Table 22
Configuration of Call Server data blocks (cont'd.)

Datablock	Overlay	Element Manager
Electronic Switched Network 3	90	Yes Dialing and Numbering Plans > Electronic Switched Network
Multi-Tenant Service	93	No
Multifrequency Signaling	94	No
Call Party Name Display	95	Yes Customers > Customer Edit > Call Party Name Display
Configuration Record 2	97	Partial System > Superloops
Ethernet and Alarm Management	117	Yes System > IP Network > Zones QoS: System > IP Network > QoS Thresholds System > Alarms > SNMP System > IP Network > Network Address Translation System > Geographic Redundancy > Database Replication Control System > IP Network > Zones > Zone > Zone Basic Property and Bandwidth Management

Signaling Server

Table 23 "Signaling Server configuration" (page 85) provides a key to Signaling Server activities.

Table 23
Signaling Server configuration

Activity	Command Line Interface	Element Manager and Networking Routing Service (NRS) Manager
Configuration parameters	Partial	Element Manager: System > IP Network > Nodes: Servers, Media Cards>Configuration NRS Manager: Home > System Wide Settings Home > NRS Server Settings
NRS numbering plan	Partial	NRS Manager: Configuration > Service Domains Configuration > L1 Domains (UDP) Configuration > L0 Domains (CDP) Configuration > Gateway Endpoints Configuration > User Endpoints Configuration > Routing Entries Configuration > Default Routes Configuration > Collaborative Servers

Voice Gateway Media Cards

Configuration of the Voice Gateway Media Cards is supported by the Command Line Interface (CLI) and Element Manager. For more information, consult *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Element Manager

Element Manager can take the place of certain configuration tasks at the CLI. Element Manager provides a way to execute CLI commands on each of the core components, indirectly and remotely through a web browser. It also provides access to command options.

IP Line (IP Telephony)

On CS 1000 systems, Voice Gateway Media Card and Signaling Server parameters are configured using Element Manager. For more information on IP Line, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

IP Peer Networking / NRS

The IP Peer Networking parameters that exist on the Call Server and Voice Gateway Media Cards are configured using Element Manager. NRS parameters are described and implemented in *Network Routing Service: Operations (NN43001-564)*..

Fault Management

Command Line Interface

The following sections describe Command Line Interface (CLI) fault management capabilities.

Call Server

All fault clearing procedures are in *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)*

Alarm monitoring and management

System alarms are based on various fault monitors and indicators. The category of the alarm indicates the severity of the system failure:

- A **major** alarm requires immediate action. It indicates a fault that seriously interferes with call processing.
- A **minor** alarm requires attention, but not necessarily immediate attention. It indicates the system hardware or software has detected a fault requiring attention.
- A **remote** alarm may require attention. It is an optional extension of a major alarm to another location, such as a monitoring or test center, or to an indicator, such as a light or bell.

System alarm clearing

System alarms notify the user when the alarm condition has been cleared.

Managing system alarms consists of the following steps:

- monitoring problem conditions
- isolating problem conditions
- diagnosis
- corrective actions
- verify that corrective actions are effective

System reporting

Diagnostic software programs monitor system operations, detect faults, and clear faults. Some programs run continuously and some are scheduled.

Diagnostic programs are resident or non-resident. Resident programs, such as the Error Monitor and Resident Trunk Diagnostic, are always present in system memory. Non-resident programs are called overlay programs or loads. They are identified by a title and a number preceded by the mnemonic for load (for example, Trunk Diagnostic—LD 36).

Overlay programs, such as the Input/Output Diagnostic and Common Equipment Diagnostic, are used as Midnight and Background Routines or for interactive diagnostics. Overlays are loaded from the system disk and are run as scheduled or upon request.

See *Software Input/Output: Maintenance (NN43001-711)* for detailed information on all diagnostic programs.

Hardware faceplate displays

The faceplates on some circuit cards include Light Emitting Diodes (LEDs) or maintenance displays. These devices provide hardware status and fault information.

The LED on the faceplate of a circuit card gives a visual indication of the status of the card or of a unit on the card, as follows:

- When a green LED is steadily lit, it indicates the card is operating normally.
- When a green LED is off, it indicates the card is disabled or faulty.
- When a red LED is steadily lit, it indicates the card or a unit on the card is disabled or faulty.
- When a red LED is off and power is available to the card, it indicates the card is operating normally.

For more information on LEDs, see *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)*.

Maintenance displays on circuit cards present hexadecimal or text codes that indicate sysload status, component faults, or self-test codes. The particular codes presented vary by circuit card.

All codes received on common equipment displays are recorded in the System History File.

To interpret maintenance display codes, refer to *Software Input/Output: System Messages (NN43001-712)*.

System messages

System messages, along with indicators such as maintenance display codes and LED indicators, identify faults in the system.

System messages are codes with a mnemonic and number, such as PWR0014. The mnemonic identifies an overlay program or a type of message. The number identifies the specific message. Table 24 "System message format example" (page 88) gives an example of the format for a system message.

Table 24
System message format example

System message: PWR0014	Interpretation
PWR	This message (generated by the system monitor) indicates power and temperature status or failures.
0014	This message means the system monitor failed a self-test.

See the *Software Input/Output: Administration (NN43001-611)* for a description of all maintenance commands, and the *Software Input/Output: System Messages (NN43001-712)* for the interpretation of all system messages.

Signaling Server

The Signaling Server has resident system reports that are available at the CLI.

Voice Gateway Media Cards

Voice Gateway Media Cards have faceplate displays that indicate the card status. “Hardware faceplate displays” (page 87) Resident system reports exist on Voice Gateway Media Cards. For more information, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

The IP Line error log contains error conditions as well as normal events. Some of the error conditions can be severe enough to raise an alarm through SNMP traps. Use the **`LogFilePut`** command to download an error log.

You can monitor voice packet loss using the following commands at the IPL> CLI:

- **`vgwPLLog 0|1|2`**: this command enables the packet loss monitor.
- **`itgPLThreshold xxx`**: this command sets the packet loss logging and alarm threshold.

Element Manager

Element Manager supports configuration of SNMP. Configuration of SNMP by Element Manager at the system level propagates upward to the SNMP Profile Manager. Changes made in Element Manager apply to all CS 1000 elements.

The SNMP parameters are grouped in three logical groups in the SNMP Configuration Web page:

- System Info
- Management Information Base Access
- Alarm

For detailed information about SNMP,*Communication Server 1000 Fault Management - SNMP* (NN43001-719).

Accounting

Command Line Interface

The system supports the generation of Call Detail Recording (CDR) records, which can be enabled using LD 21 (see *Software Input/Output: Administration (NN43001-611)*).

CDR

The Call Detail Recording (CDR) feature provides information on incoming and outgoing calls for accounting and administration purposes. CDR records are assembled by software and sent through Serial Data Interface (SDI) ports to any EIA RS-232-compatible output or storage device. Teletype writers (TTY) and printers are examples of output devices. Single-port or Multi-port CDR storage systems are examples of storage devices.

All calls generate, at a minimum, single call records. Unmodified calls generate a Normal record. Modified calls generate Start, Transfer and End records. Multiple call records can be generated for calls which are impacted by certain features.

For more information on activation of CDR, CDR types, and fields, refer to the *Call Detail Recording: Description and Formats (NN43001-550)*.

Element Manager

Element Manager does not support any billing applications.

Performance monitoring

This section lists performance-monitoring tools available through various interfaces to the system.

For more information about maintenance activities on the CS 1000 system, see the Maintenance NTPs. For more information about maintenance on the Voice Gateway Media Cards, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Command Line Interface

This section describes performance monitoring options available at the Command Line Interface (CLI).

Call Server

On the Call Server, LD 2 is the overlay used to configure traffic report schedules, as described in *Software Input/Output: Administration (NN43001-611)*.

One Traffic Log File can be specified per system. All system-generated traffic reports are recorded in this file rather than the History File, making these reports more accessible. The contents of this file survive a sysload.

Element Manager

This section describes performance monitoring options available through Element Manager.

Call Server

Use Element Manager to configure parameters that trigger performance using Element Manager. Users can view raw data through the most recent records available.

Signaling Server

Use Element Manager to view the traffic level history through the Signaling Server-specific performance monitoring. The system stores a log of the number of registration and admission requests handled per hour. The traffic level history is tracked on a per-registered-endpoint basis.

Use Element Manager to perform the following performance monitoring functions:

- Monitor the state of endpoint registrations: This option displays the call signal and RAS IP addresses of all currently registered endpoints. If an endpoint provides multiple alias addresses or vendor information in the RRQ message, this is also shown.
- View the traffic level history: This option displays a log of the number of registration and admission requests handled per hour is kept. The traffic level history is tracked on a per registered endpoint basis.
- View the bandwidth usage history: This option displays a log of the bandwidth requested per hour, as recorded by the NRS.
- View the alarm and exception log histories for the NRS and Signaling Server: This option displays alarm and exception log histories and of selected components. For more information, see “Fault Management” (page 86)

For more information about the NRS and Element Manager, see the *IP Peer Networking Installation and Commissioning (NN43001-313)* and *Element Manager System Reference - Administration (NN43001-632)* guides.

Communication Server 1000 logs

This section provides information about Communication Server (CS) 1000 log files.

Communication Server 1000 log file descriptions

Call Server log files (VxWorks and Linux Co-resident Call Server)

Report log

The VxWorks based Call Server and Linux based Coresident Call Server logging infrastructure can generate up to 50 1-MB files that are persistent and archived on a circular basis. When the size of the currently-opened file is reached, the file is closed and a new report file is created. Once the fiftieth file is full, the infrastructure begins writing over the oldest log file. The 50 files are stored in the /e/rpt directory and are named LOG000XX.RPT (XX = 00 to 49).

The SSC-based Call Server application has a single Report Log infrastructure with a 667 record circular log. The Report log directory is located at the 'c:/u/rpt' directory on the SSC-based Call Server.

The CPP-based and SSC-based Call Server logs are accessible through PDT Level 1 on the Call Server CLI or through Element Manager. Report file browsing utilities (RD Tools) are available at the CLI and Element Manager that enable the system administrator to browse through the files. The Report log is a Binary file.

The logs contain a large collection of Call Server application, OS and system events, which can include very detailed debugging information from various software registers and the CPU stack. Some examples of events that are recorded in the Call Server Report log include:

- Initializations
- ELAN events
- Midnight Routine results
- Media Gateway/Signaling Server link events
- Health count - redundancy state changes (applicable system types)
- Hardware events

- Backup events
- Security events (Login/Logout/Password changes)
- Patch insertion - state changes
- Core dumps

History File log

The log is a circular file that resides in protected memory and has a size that can be defined by the System Administrator (maximum size: 65 Kb). The file is non-persistent, which means the contents of the file are lost if the Call Server has a cold start. The contents of the log survive a CPU switchover and warm start (INI). The file is accessible through LD 22 on the Call Server CLI or through a rlogin session. LD 22 log-browsing utilities (VHST) are available to search through the log.

The History log can contain information related to Call Server access (including username, port accessed, login/logout time stamps, list of Overlays accessed and session duration) and can optionally be configured to archive Service Change messages, maintenance and software error messages, Malicious Call Trace messages, and Traffic Reporting data through LD 17 administration.

System Event log

The System Event log is a Call Server CLI-accessible logging infrastructure. It provides centralized access to the same type of information that is archived in the History File log and the Report log (at a non-debug informational level). The System Event log is a persistent file that resides on the Call Server hard drive. The size can be defined up the system administrator (maximum size: 2000 events). The file is accessible through LD 117 on the Call Server CLI. There are also log-browsing utilities available to search through the System Event log in LD 117.

The System Event log contains a large collection of Call Server, OS, and system events. Some examples of events that are recorded in the Call Server Report log are:

- System Access Events
- ELAN events
- Midnight Routine results
- Media Gateway/Signaling Server link events
- Health count - redundancy state changes
- Hardware events

- Backup events
- Application error messages

Application Message Trace Tool log

The Application Message Trace Tool log is an optional logging file infrastructure. It enables support personnel to archive the results of any LD 96-enabled D-Channel Message Trace Utility events. The DCH Message Trace log is a persistent circular file that resides on the Call Server hard drive and has a size of 1 MB. The file is accessible through the Call Server PDT Level 1 CLI.

Traffic File log

One Traffic File log can be specified for each system. All system-gen erated traffic reports are recorded in that log file rather than the History File. The log is a circular file that resides in protected memory and has a size that can be defined by the System Administrator (maximum size: 64 Kb). The file is archived in protected memory and is non-persistent, which means the contents of the file are lost if the Call Server does a cold restart. The contents of the log survive a CPU switchover or warm start (INI). The log file is accessible through LD 22 on the Call Server CLI or through a rlogin session. Log-browsing utilities (VHST) are available to search through the log.

TTY File log

The CS 1000 Multi-User Login feature logs all system administrator activity executed on a specific TTY or Pseudo-TTY console interface on the CS 1000 Call Server. The log is a circular file that resides in protected memory and has a size that can be defined by the System Administrator (maximum size: 64 Kb). The log file is non-persistent, which means the contents of the file are lost if the Call Server does a cold restart. The contents of the log survive a CPU switchover or warm start (INI). The log is defined in LD 17 (TTYLOG) under the ADAN interface and is accessible through LD 22 on the Call Server using CLI or an rlogin/telnet/SSH session. Log-browsing utilities (VHST) are available to navigate and search through the log.

The log can record data related to all Call Server OAM tasks initiated by the system administrator up to the limit of the log file for the TTY/PTY port.

Media Gateway Controller, DSP daughterboards, and Voice Gateway Media Card

Report log

Media Gateway Controllers (MGC) and the associated DSP daughterboards, as well as the MC32S Voice Gateway Media Card share a common logging infrastructure. The logging infrastructure is very similar to the one shared by the Call Server and the VxWorks-based Signaling Server, with the primary difference in that it supports a maximum of twelve 1-MB log files. The twelve files are stored in the /e/rpt directory and are named LOG000XX.RPT (XX = 00 to 12). The file rotation mechanism is the same as the Call Server and Signaling Server Report logs.

The files on both platforms are accessible through Element Manager and are accessible through CLI at PDT Level 1 on the Voice Gateway Media Card and through CLI, LDB level 1 on the MGC/DSP daughterboard platforms. There are report file-browsing utilities (RD Tools) available at the CLI and Element Manager. The Report log is a binary file.

The logs contain a large collection of Voice Gateway (VGW) and Terminal Proxy IP Telephony Application and Platform events. Some examples of events that are archived include:

- ELAN events
- Access/Logon events
- Call Server registration
- IP Phone registrations (MC32S)
- Firmware downloads (MC32S)
- VGW registrations
- Redundancy state changes
- Hardware events
- Patch Changes
- Configuration file synchronization.

Operational Measurement logs

The MGC/DSP daughterboard and MC32S generate a collection of OM reports every hour to an OM log file. At midnight, the OM log file is closed and a new OM report log is opened. OM reports are generated on a per-card basis, with the eight most recently-developed reports archived in a round-robin fashion in the /u/om directory. The report file is in a .csv format and is named omreport.xxx (xxx = sequence number) The OM log files on both platforms are accessible through Element Manager and at the OAM Level CLI of the MGC/DSP daughterboard and MC32S.

The logs contain statistics on the number of:

- incoming and outgoing calls
- call attempts
- calls completed
- QoS Statistics
- total holding time for voice and fax calls.

The OM data is applicable to the LTPS IP Telephony applications (MC32S Only) and VGW.

Voice Gateway Media Cards

SYSLOG log

Voice Gateway Media Cards share a common logging infrastructure. The logging infrastructure is based on the SYSLOG function and supports a maximum of four 16 KB log files. The four files are stored in the /C:/Log directory and are named SYSLOG.X (X = 0 to 3). The files on both platforms are accessible through Element Manager and CLI at the IPL> Level interface on the Voice Gateway Media Cards. The file is in a text format. Syslog forwarding capability is not available.

The logs contain a large collection of Voice Gateway (VGW) and Terminal Proxy IP Telephony Application and Platform events. Some examples of events that are archived include:

- ELAN events
- Access/Logon events
- Call Server registration
- IP Phone registrations
- Firmware downloads
- VGW registrations
- Redundancy state changes
- Hardware events
- Patch changes
- Config file synchronization.

History File log

Voice Gateway Media Cards have a History File log that is created when the card starts. The text file is called audit.his and is stored in the /C:/LOG directory. This file contains a list of the problems found and the actions taken by the maintenance audit. The audit.his file has a fixed size of 4096 bytes. The most recent records in the file overwrite the oldest records, with newest events appearing at the beginning of the file. A record in the file is a one-line string with maximum size of 256 characters. The file can be accessed through the IPL> CLI.

Operational Measurement logs

Voice Gateway Media Cards generate a collection of OM reports every hour to an OM log. At midnight, the OM log file is closed and a new OM report log is opened. OM reports are generated on a per-card basis, with the eight most recently-developed reports archived in a round-robin fashion in the /C:/OM directory. The report file is in a .CSV format and is named omreport.xxx (xxx = sequence number). The OM log files on both platforms are accessible through Element Manager and at the IPL> Level CLI of the Voice Gateway Media Cards.

The logs contain statistics on the number of:

- incoming and outgoing calls
- call attempts
- calls completed
- QoS statistics
- total holding time for voice and fax calls.

The data archived is applicable to the VGW and LTPS IP Telephony applications.

Linux base operating system

The Linux base operating system (OS) contains a collection of logs that are primarily located in the /var/log directory. In addition, some of the CS 1000 hosted IP Telephony applications have a directory within /var/log for each specific application log file.

Many of the log files in the /var/log directory have a naming convention with numbers inserted into the file name. The numbers are created when the log files are rotated using the Linux logrotate utility. The logrotate package generates a cron task that automatically rotates log files according to the /etc/logrotate.conf configuration file. By default, logrotate is configured to rotate every week and save four weeks of previous log files. The operation described is applicable for the Common Linux OS log files and the CS 1000 Linux base log files.

Common Linux OS logs

The Common Linux OS logs are rotated by using the logrotated mechanism and archived in the /var/log/ directory. These logs are persistent on the hard drive, but are not part of any system-level back-up utility. The files and directory are “root” owned and accessed. More detailed information on these Common Linux logs can be found on the Web or in a Redhat Enterprise Linux technical book.

The following are some examples of Common Linux OS logs:

1. /var/log/anaconda.log - Anaconda is the installation program used by Red Hat Enterprise Linux. Anaconda handles the basic setup and configuration of the system as well as installation of packages for the system
2. /var/log/cron.log - Cron daemon logs
3. /var/log/faillog - a Linux database that maintains login failure counters and limits. Contents are accessed using the Linux utility /usr/bin/faillog
4. /var/log/dmesg - Kernel startup/bootup log. Output of the Linux utility /bin/dmesg which helps users to print out their bootup messages
5. /var/log/lastlog - database of times of previous user logins. Contents are accessed using the Linux utility /usr/bin/lastlog
6. /var/log/messages - the messages log is the core system log file. It contains the boot messages when the system came up as well as other status messages as the system runs. Errors with IO, networking, and other general system errors are reported in this file. Other information, such as when someone becomes root, is listed her. If services are running, you can watch the action in the messages file.
7. /var/log/rpmpkgs -RPM package installation log
8. /var/log/secure - authentication messages, xinetd services
9. /var/log/snmp.log - log output from the snmp agent
10. /var/log/xferlog - SFTP daemon log
11. /var/log/mgetty.log.* - modem/fax log
12. /var/log/ppp/connect-errors – PPP connection log

CS 1000 application logs

All CS 1000 applications make use of the Linux syslog facility. The log files are stored in the “/var/log/nortel/” directory.

Application logs use Linux syslog implementation to log the messages. These application are:

- LTPS
- SIP Line Gateway
- SIP Signaling Gateway
- NRS Routing Bundle (NCS, H323 GK, SIP Redirect Server)
- Management Bundle
- Linux base log
- Co-res Signaling server
- Other Nortel specific application logs

All applications using the Syslog facility use the logrotation mechanism. Logrotation is run every 24 hours to validate if it is necessary to rotate log files. If any of log file described below exceeds 5 Mb, then the log is archived in the “/var/log/nortel/old_logs/” directory. When there are five copies of old files, then the oldest log is deleted and overwritten first. These logs are persistent on the hard drive but are not part of any system level backed-up utility.

The following are some examples of CS 1000 Linux base files and directories that are Nortel-owned and accessed:

1. /var/log/nortel/linuxbase.log – Linux base log including boot messages
2. /var/log/nortel/ncgl_patch.log – NCGL patcher logfile (verboseness level controlled through /etc/slgtrace.d/tap_pa configuration file (template found in /tmp/slgtrace.tap_pa)
3. /var/log/nortel/nortel_snmp.log – Nortel SNMP logfile
4. /var/log/nortel/nortel_solid.log – Nortel Solid
5. /var/log/nortel/nrs.log – NCS, GK logfile
6. /var/log/nortel/ss_common.log - Signaling Server applications such as LTPS, SIP GW, and H323GW
7. /var/log/nortel/OAM - Security and OAM audit Logs
8. /var/log/nortel/callserver.log - logs for Co-resident Call Server

All application logs are stored on the Linux base server hosting the CS 1000 application. You can view the logs using the Log viewer that is available in the Base Manager or via the CLI of the host server.

The Syslog Forwarding feature is not available for the CS 1000 application logs listed above

Ten percent of the total disk space is allocated for the CS 1000 application logs.

Unified Communications Management

Operation, Administration, and Maintenance Transaction Audit Logs and Security Logs

The primary purpose of the Operation, Administration, and Maintenance (OAM) Transaction Audit Logs feature is to securely maintain an audit trail of all system administrator OAM activities. The security-specific events OAM logs and the Security logs are archived centrally on the Primary UCM Security Server within the CS 1000 management framework, with the ability to forward the log files to external Operational Support System (OSS) using SYSLOG.

In order to be effective, security audit logs must contain sufficient information for after-the-fact investigation or analysis of security incidents. These audit logs provide a means for accomplishing several security-related objectives including individual accountability, reconstruction of past events, intrusion detection and problem analysis.

The centralized UCM primary security server has a log viewer tool to view the Security and Operation, Administration, and Maintenance (OAM) related audit logs. When logged on as a security administrator, the following functions can be performed:

- Filter the log based on the query string and event types.
- View the log for a specific date.
- Configure the remote SYSLOG server for forwarding audit logs in real time to the third party Operational Support System (OSS)
- Export the log as a comma-separated value (csv) file.

The OAM audit log traces all administrative activity when using web based management applications. The management applications include the following:

- Unified Communications Management
- Element Manager (including Phone Provisioning)
- Network Routing Service Manager
- Subscriber Manager
- Web Services
- Base Manager
- Patching Manager

Log storage

Operation, Administration, and Maintenance (OAM) and Security Logs are stored on the Linux machine where they are generated. In order to provide better access control and to maintain an audit trail of all system administrator activities and security related events, the OAM and Security logs from the backup and member servers are forwarded to the UCM primary security server as the centralized storage location. OAM audit logs are provided for the CS 1000 management applications running on a Linux platform to record security, operational, configuration and maintenance events. The OAM log files security.log and oam.log are archived in the /var/log/nortel/OAM directory of the primary UCM server

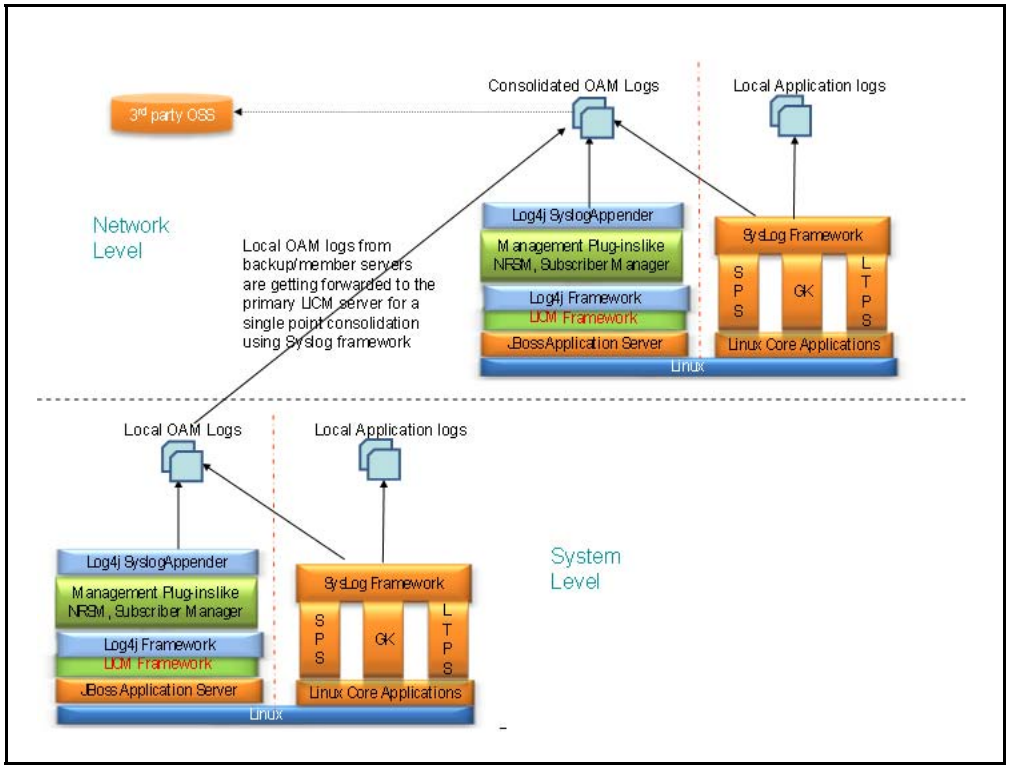
Logging Architecture

The OAM and Security logs generated and stored in each backup and member Linux server are forwarded to the primary UCM server for consolidation. During software installation the Syslog daemon on these servers are configured to forward the OAM logs to the centralized Syslog daemon running on the primary UCM server.

All the OAM and Security logs from the backup/member UCM server will be forwarded in real-time to the primary UCM server, only after the Log Configuration is enabled in the backup/member UCM server, through the Base Element Manager Logs link

The architecture of this log forwarding mechanism is shown in the following figure.

Figure 13
Logging Architecture



OAM Audit and Security Log Rotation

The OAM audit log files are configured to have a log rotation of 30 days. The logs are rotated on a daily basis (for example, there are two log files (oam.log and security.log) created on a daily basis). The log files can exist for a maximum of 30 days; therefore, at a maximum, there could be 60 files in total in the system.

> ***Note:*** If you need to store more than 30 days history of OAM logs, forward the logs to external archiving using the syslog forwarding feature.

When the two log files are created, the creation date is appended to the log file name. The archived files for the oam.log and the security.log are stored in compressed format and the naming convention for archived files is xxx.log-YYYYMMDD.gz

Log Viewer Tool

The centralized UCM Primary Security Server has the Log viewer tool to view the two log types. This tool provides the following facilities:

- User can filter the logs based on the query string and also on the event types.
- User can view the set of OAM audit logs that got generated on a particular date.
- User can configure to forward the logs in real-time to 3rd party OSS.
- User can export the logs as a CSV file.

Any number of users with the security administrator role can access the Log viewer tool simultaneously.

Note: OAM and Security log files smaller than 5 MB can only be viewed from the Logviewer interface. If the log file is larger than 5 MB, a link to export and download the file appears. A 5 MB log file can record approximately 50000 log events.

Logging Events

The log files viewed by using Logviewer interface are broadly classified as:

1. OAM Logs: The OAM related logs are stored in two different files based on the type of logging event as given below:
   - Security Logs: The OAMTransaction Audit and security event logging feature consolidates all the security events that take place within any CS 1000 system element into security.log file. Examples of security events include:
     - Security policy changes
     - Logon success and failures from CLI / Web interfaces
     - Certificate changes
     - User Account Creation and Illegal (failed) Login Events
     - Any OAM security event where security administrator privilege (or flag) is enabled or required
2. OAM Audit Logs: All the audit related logging events consolidated into oam.log file include the following events:
   - Operational Events: This captures the query for status and enabling or disabling resources.
   - Linux CLI messages

— Configuration Events: This captures all the feature or functional provisioning and modifications.

— Maintenance Events: This captures all the upgrades, backups, restores and patching.

Log format

CS 1000 log files contain the following fields:

- Priority
- Time generated
- Time reported
- Host name
- Message

Table 25 "CS 1000 log file fields" (page 103) describes each field.

Table 25
CS 1000 log file fields

Field name	Description
Priority	The priority of the syslog message.
Time generated	The time at which the event occurred.
Time reported	The time at which the syslog message arrived at the consolidation point.
Host name	The host name of the source server. ***Note:*** If the host name is not available, this field displays the IP address of the source server.
Message	Message contains the following information: • User name: the Unified Communications Management (UCM) user name of the administrator or the machine that invokes the request. • Remote network device identity: a remote network device identity, managed element IP address, or X.500 object identifier. • Severity: syslog message level. • Message string: log message content. • Result: success or failure of the action.

The following list shows sample log messages:

- local3.info Aug 26 12:34:27 Aug 26 12:34:27 hpss1 admin: 192.168.55.173: Info: Restart SIP Proxy Server – SUCCESS
- local3.alert Aug 26 12:34:27 Aug 26 12:34:27 hpss1 admin: 192.168.55.173: Alert: Restart Gatekeeper service – FAIL

UCM Linux base OS security logs

UCM Linux base supports two types of audit logs

1. Administration audit logs, which track administration activities such as create/read/update/delete elements, users, roles, certificate, security policies. These logs are generated from OpenSSO authentication and authorization services when handling requests from SSO sessions.
2. Operational audit logs, which track operational activities such as user logon, logout, or access control policy evaluations. These logs are generated from OpenSSO authentication and authorization services when handling requests from SSO sessions.

Utilities

This section provides information about management utilities available on CS 1000 and Meridian 1 systems.

Command Line Interface

This section describes utilities available from the Command Line Interface (CLI) .

Call Server

For more information about utilities available on the Call Server and Media Gateway CLI, refer to*Software Input/Output: Administration (NN43001-611)*, and *Software Input/Output: Maintenance (NN43001-711)*.

The Equipment Datadump (EDD) utility is available in LD 43 on the Call Server. EDD backs up and synchronizes copies of the customer database to the associated Media Gateways. Database backup and restore is performed using the **Utilities** menu from the Software Installation Program.

To configure the system date and time, you can either set it during system installation, or using LD 2. This task is discussed in “Configuration of data blocks and components” (page 80).

Corporate Directory is available from LD 11.

Element Manager

The following Call Server Tools can be accessed through Element Manager:

- Backup and Restore
- Call Server Initialization
- Date and Time
- Logs and Reports

This section describes utilities available in Element Manager. For more information about Element Manager utilities, refer to *Element Manager System Reference - Administration (NN43001-632)*.

Call Server Backup

The Call Server Backup function invokes a datadump and writes the Call Server data to the primary nd internal backup drives. The Backup function performs the same task as the CLI command EDD in LD 43.

Call Server 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 RBI command in LD 43.

Date and Time

The Date and Time function enables modification of the system's current time and date using Element Manager. This page also allows the configuration of Network Time Protocol (NTP) and Network Time Synchronization (NTS) parameters. This also allows configuration of Daylight Savings Time.

The date and time management covers the configuration of time synchronization options, as well as the setting of the actual date and time, and time zone related settings. An important concept is that there is a recommended configuration for any elements that are part of a CS 1000 system (these are running CS 1000 applications, such as CS, SS, SIPL, PD).

Timezone offsets for distributed phone subscribers is separately configurable through the Element Manger Branch Office zone configuration. In order to ensure that the configuration for a CS 1000 system is consistent, the configuration must be done using Element Manager.

The purpose of system-level coordination of the operating system date and time configuration for all elements of a single CS 1000 system is to facilitate the interpretation of system event and error messages generated by different elements.

The CS 1000 system level date and time management in Element Manager allows the configuration of Network Time Protocol (NTP) and Network Time Synchronization (NTS). The NTS client and NTP usage are mutually exclusive options for the CS 1000 system. A Call Server may be designated as the NTS master and utilize NTP to synchronize its own time.

For any other Linux servers that are not part of a CS 1000 system, configuration is done using Base Manager of UCM. See, *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Configuration of time synchronization options performed from Element Manager overrides those previously performed by CLI, Base Manager, or the install tool on all system elements. Conversely, if changes are attempted later on at the individual element level that may interfere with the system time synchronization options chosen at the system level using Element Manager.

Nortel recommends that you use the ELAN interface for all NTP communication within a system. This would be to communicate to CS 1000 NTP primary and secondary servers. The CS 1000 NTP primary and secondary servers would normally communicate with external NTP clock sources using their TLAN connections. If TLAN is not available, then ELAN would be used. In all cases, it is necessary to ensure that appropriate routing is in place for communication between devices. This applies for communication to external sources and also for communication with CS 1000 NTP primary and secondary servers if the ELAN network interfaces of devices are on different subnets.

For more information about Date and Time, refer to*Element Manager System Reference - Administration* (NN43001-632).

Logs and Reports

The following logs and reports can be accessed under the Tools link of Element Manager:

- Call Server Reports
- Equipped Feature Packages
- Peripheral Software Version Data
- System License Parameters
- Operational Measurements

- System Traffic
- Customer Traffic
- Traffic Parameters
- Quality of Service
- Bandwidth Management
- Individual Traffic Measurement

Maintenance

Table 26 "Maintenance activities" (page 107) represents a non-exhaustive list of maintenance tasks that can be performed with CS 1000management.

Table 26
Maintenance activities

System component	Activity	Command Line Interface	Element Manager
Call Server	Status	See Table 27 "Maintenance overlays" (page 108).	System > IP Network > Nodes: Servers, Media Cards > Maintenance and Reports
	Patches	Yes	System > Software > Servers, Media Cards PEPs
Signaling Server	Status	Partial	System > IP Network >
	Backup/ Restore		NRS > Tools > Database Backup NRS > Tools > Database Restore
	Software download		System > Software > File Upload>
	Patches download and activation		System> Software> Servers, Media Cards PEPs

Table 26
Maintenance activities (cont'd.)

System component	Activity	Command Line Interface	Element Manager
Voice Gateway Media Card	Status / Error messages	Partial	System > IP Network > Nodes: Servers, Media Cards > Maintenance and Reports> Node> Voice Gateway Media Card> SYSLOG
	Patches download and activation	Partial	System > IP Network > Software > Servers, Media Cards PEPs
	Loadware and firmware versions and upload	Partial	System > IP Network > Software> File Upload
	IP Line and IP Phone maintenance and diagnostics	LD 32—See Table 27 "Maintenance overlays" (page 108).	

For maintenance activities on the CS 1000 systems, refer to the Maintenance NTPs. For maintenance commands specifically available through Element Manager, refer to *Element Manager System Reference - Administration (NN43001-632)*.

Call Server activities

The datablocks and activities listed in Table 27 "Maintenance overlays" (page 108) are available on the Call Server.

Table 27
Maintenance overlays

Activity or Datablock	CLI	Element Manager
Template Audit	LD 1	No
Network and Signaling Diagnostic	LD 30	System> Maintenance> Network and Signaling
Telephone and Attendant Console Diagnostic	LD 31	No
Network and Peripheral Equipment Diagnostic	LD 32	System> Maintenance> Network and Peripheral Equipment
Peripheral Equipment Diagnostic for 1.5 Mb/s RPE and Fibre Remote IPE	LD 33	No

Table 27
Maintenance overlays (cont'd.)

Activity or Datablock	CLI	Element Manager
Tone and Digit Switch and Digitone Receiver Diagnostic	LD 34	Partial System> Maintenance> Tone and Digit Switch
Trunk Diagnostic	LD 36	System> Maintenance>> Trunk
Input/Output Diagnostic	LD 37	Partial System> Maintenance> Input/Output
Conference Circuit Diagnostic	LD 38	No
Intergroup Switch and System Diagnostic	LD 39	System> Maintenance> Intergroup Switch and System Clock
Call Detail Recording Diagnostic	LD 40 LD 42	No
Equipment datadump Database backup and restore	LD 43	Partial Tools > Backup and Restore > Call Server
Software Audit	LD 44	No
Background Signaling and Switching Diagnostic	LD 45	Partial System> Maintenance> Background Signaling and Switching
Multifrequency Sender Diagnostic for Automatic Number Identification	LD 46	System> Maintenance> Multifrequency Sender
Link Diagnostic	LD 48	Partial System> Maintenance> Link
Intercept Computer Update	LD 51	No
2.0 Mb/s Remote Peripheral Equipment Diagnostic	LD 53	Not applicable
Multifrequency Signaling Diagnostic	LD 54	System> Maintenance> Multifrequency Signaling

Table 27
Maintenance overlays (cont'd.)

Activity or Datablock	CLI	Element Manager
Digital Trunk Interface and Primary Rate Interface Diagnostic	LD 60	System> Maintenance> Digital Trunk Interface and Primary Rate Interface
Message Waiting Lamps Reset	LD 61	No
1.5 Mbps Remote Peripheral Equipment Local End Diagnostic	LD 62	Not applicable
Conversion	LD 66	Not applicable
Digital Trunk Maintenance	LD 75	System> Maintenance> Digital Trunk
Manual Print	LD 77	No
Call Trace	LD 80	Partial System> Maintenance> Call Trace
Automatic Trunk Maintenance	LD 92	No
D-Channel Diagnostic	LD 96	Partial System> Maintenance> D-Channel
Ethernet and Alarm Management	LD 117	Partial System> Maintenance> Ethernet and Alarm Management
Core Common Equipment Diagnostic	LD 135	Partial System> Maintenance> Core Common Equipment
Core Input/Output Diagnostic	LD 137	Partial System> Maintenance> Core Input/Output
Customer Configuration Backup and Restore	LD 143	Tools > Backup and Restore > Call Server

Command Line Interface

Maintenance programs perform hardware and software diagnostics. They also enable, disable, and check hardware status.

Call Server and Media Gateway

The following maintenance activities are supported:

- **Background.** When users are not running maintenance overlays, special maintenance programs run continuously in the background to monitor system performance. These programs detect system discrepancies before they begin to affect service. When there is sufficient CPU capacity, background routines also execute a set of overlays to ensure the integrity of the system.
- **Midnight or Daily Routines.** In addition, a set of maintenance programs runs automatically once a day, usually at midnight. These are called daily or midnight routines. Results of selected tests run by these routines appear on the TTY. The system prints a banner page to indicate the beginning and ending of each daily routine. The content of the banner page is as follows:

  ```
  DROLXXX <Overlay Mnemonic> <LD xx> <BEGIN, END><Time stamp>
  ```

  The following is an example of the banner page for a daily routine:

  ```
  DROL000 NWS LD 30 BEGIN 00:35 23/1/92
  .
  .
  .
  DROL001 NWS LD 30 END 00:42 23/1/92
  ```

- **Manually Loaded.** Most other maintenance programs use a command/action/response format. When you enter a command, the system performs the requested action and responds with the result.

Refer to *Software Input/Output: Maintenance (NN43001-711)* for the complete list of maintenance programs, as well as their prompt/response sequences.

System database backup and restore

The **Utilities** menu of the CS 1000Installation program can be invoked at any time from the command line. Database archive and restore procedures are explained in the *Upgrades* NTPs.

A LD 43 EDD synchronizes a copy of the customer database from the Call Server to the Media Gateways.

Backup and restore

The master copy of the IP telephony node files are stored on the Call Server. Each Voice Gateway Media Card has a copy of these files. As a result, it is not necessary to backup or restore the IP telephony node files found on the Voice Gateway Media Cards.

To restore information to a Voice Gateway Media Card, use the **`configFileGet`** command as described in *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Signaling Server CLI

A set of CLI commands is available for the Signaling Server. For CLI commands on the Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Backup and restore

The master copy of the IP Telephony node files are stored on the Call Server. As a result, it is not necessary to back up or restore the IP Telephony node files found on the Signaling Server. For more information, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Element Manager

To have access to the patching feature, PDT access is given at the UCM level when Radius Authentication is turned on. Patches can be downloaded from the Nortel web site using any web browser.

From Element Manager, you can upload and place patches into service on the Call Server, Media Gateways, and the IP telephony components. See *Element Manager System Reference - Administration (NN43001-632)*.

You do not need to receive notification and software media from Nortel to perform routine maintenance and upgrade tasks. All software and patches are available from the Nortel Software Download web site. Instructions for using the web site are found in *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Call Server

Patching of the Call Server can be performed with Element Manager. For more information about patching, see *Element Manager System Reference - Administration (NN43001-632)*.

A datadump can be invoked from the **Tools » Backup and Restore » Call Server Backup and Restore** menu in Element Manager. See *Element Manager System Reference - Administration (NN43001-632)* and *Signaling Server IP Line Applications Fundamentals* (NN43001-125) for more information.

Voice Gateway Media Card

Patching the Voice Gateway Media Card occurs through patching IP telephony components.

You can also upgrade the Voice Gateway Media Card and IP Phones as a maintenance activity when new releases of software are available. See the following NTPs for the procedures:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures (NN43011-459)*
- *Communication Server 1000E Upgrades (NN43021-458)*
- *Communication Server 1000E: Upgrade Procedures (NN43041-458)*

Limited Access to Overlays

Use Limited Access to Overlays to restrict user access to specific programs and data. You can define up to 100 login passwords in the configuration record (LD 17), each with its own set of access restrictions. For each of these Limited Access Passwords (LAPW), define the level of access that the password provides. You can control the following:

- access to specific overlays
- modification of specified customer data
- access to specific tenant numbers
- access to Speed Call lists through the print routines in LD 20
- access to the Configuration record (CFN) in LD 17:
  - no access at all
  - changing a user's own password only
  - full access to configuration information
- access through the Print Only option:
  - access to administration overlays that contain print commands, with use limited to the print commands in those overlays
  - full access to all print routines: LD 20–22 and LD 81–83
  - access to system commands in Traffic LD 2 only to users with access to all customers. Customer-defined commands are accessible according to the customer numbers defined for each password.

Only the user of the highest level password – PWD2 – can configure or change access for other passwords. This password must be reserved for system administrators.

Implementing and using the LAPW feature does not interfere with using any existing passwords in the system. For a complete listing of the passwords currently used, refer to LD 17 (prompts PWD2, NPW1, NPW2) and LD 15 (prompts ATAC and SPWD) in *Software Input/Output: Administration (NN43001-611)*.

You must be logged in with PWD2 to associate a user name with PWD1, PWD2, and the 100 LAPW passwords. The user name can be up to 11 alphanumeric characters. Use the LNAME_OPTION in LD 17, which defaults to YES, to indicate that login names are required. When the value is YES, the system assigns the default user names listed in the table Table 28 "Default user names" (page 114), which you can change using LD 17.

Table 28
Default user names

Password	User Name
PWD1	ADMIN1
PWD2	ADMIN2
PW00–PW99	USER0–USER99

If you configure LNAME_OPTION as YES, the system accepts non-unique passwords. If you configure LNAME_OPTION as NO, the system creates a new, random password for each user, which ensures that the passwords are indeed unique.

WARNING
When you configure LNAME_OPTION as NO, the system reassigns passwords, and issues a message indicating the new PWD2 password. Without it, you are unable to change the password for any user.

Each password is valid for up to 32 customer-tenant combinations. Each combination is defined by a number designator that includes the customer number (0–99) and the tenant number (0–511).

Each Limited Access Password (LAPW) must be:

- four to sixteen characters in length with no spaces
- any combination of numbers and uppercase letters
- left-wise unique (if login name option is NO)
- different from existing passwords (if login name option is NO)

Use LD 17 to log in with PWD2 to define user access to overlays. If a user tries to access a restricted overlay, a message appears and access is denied.

You can also restrict access to certain commands within a given overlay. For example, you can specify **print only** access for a password. Users logged in with that password are restricted to print commands within an overlay. If the user attempts to use any other command, the following system message displays:

```
SCH8836 PASSWORD HAS PRINT ONLY CLASS OF SERVICE.
```

The system monitors login attempts for attempted security breaches. After a predefined number of consecutive failed login attempts, the entry point (TTY or terminal) is locked out for a predetermined time. The number of allowed failed logins, and the duration of the lockout, are configured through a service change, and are password protected. The system ignores attempted access from that entry point until the lockout timer expires.

When a lockout occurs, a report is sent to all maintenance terminals, and the next time a system administrator logs in, they also receive a report.

The system can keep an Audit Trail to record login information. The Audit Trail printout provides the following information: I/O port number, user name, and logout time. Each line in the Audit Trail printout uses the following format:

```
LOG TTY I/O# Login User Password LDs Logout
```

The Audit Trail command is explained in the table Table 29 "Format of Audit Trail (LD 22)" (page 115). An example of Audit Trail printout is shown in Table 30 "Example of Audit Trail printout (LD 22)" (page 115)).

Table 29
Format of Audit Trail (LD 22)

LOG TTY	the printout identifier
I/O#	the I/O port number from which the user logged in
Login	the time the user logged in (hh:mm)
User	the user name for this password as configured in LD 17
Password	the password used to log in
LDs	a list of overlays the user accessed
Logout	the time the user logged out (hh:mm)

Table 30
Example of Audit Trail printout (LD 22)

DAT	03/18										
LOG	TTY	#04	09:34	ADMIN2	PWD2	17	22	11	20	32	10:23
LOG	TTY	#03	11:32	USER3	PW03	20	11	20	10	20	13:34

To access the Audit Trail from LD 22 you must log in using PWD1 or PWD2.

Administrators can change the size of the Audit Trail buffer, from 50 to 1500 words (the value must be divisible by 50). When the buffer is full, new records overwrite the oldest information in the buffer (OVL401 message is sent to the active TTY and all maintenance TTYs). Printing the Audit Trail in LD 22 clears the buffer.

Operating parameters

The following restrictions apply to the use of LAPW:

- Create a configuration record in LD 17 before you enable LAPW feature.
- If you configure LNAME_OPTION in LD 17 as YES, the system assigns unique login names for all passwords, including PWD1 and PWD2. See Table 28 "Default user names" (page 114)
- If you configure LNAME_OPTION as NO, all passwords must be unique.
- Use LD 17 to configure user names and passwords. When LNAME_OPTION is changed from YES to NO, the system assigns random passwords. See warning on "page 155" (page 114) .
- Users of LAPW passwords can change their own passwords, but not their login names.
- Users and administrators cannot have more than one password defined for any one access configuration.
- With the Multi-User Login feature activated, two users can log in with the same login name/password combination. However, no two passwords can have the same login name associated with them. For example, two users could log in as ADMIN1, but ADMIN1 cannot be assigned as the user name for both PWD1 and PW01.

Feature interactions

There are no feature interactions associated with LAPW.

Feature packaging

Limited Access to Overlays (LAPW) package 164 must be enabled for LAPW to operate.

Feature implementation

To implement LAPW, you must change the Configuration Record (CFN), LD 17.

Table 31 "LD 17: Define LAPW options and passwords." (page 117) lists the responses you must enter to define LAPW options and passwords. For more information about LD 17, including an explanation of all prompts, see *Software Input/Output Administration (553-3001-311)*.

Table 31
LD 17: Define LAPW options and passwords.

Prompt	Response	Description
REQ	CHG	Change
TYPE	PWD	Password data
PWD2	xxxx	Current Level 2 password (if existing passwords will be changed)
	<cr>	<cr> indicates no changes will be made to passwords
LNAME_ OPTION	(YES) NO	Option to require name during login process
NPW1	xxxx	New level 1 login password; 4–16 characters chosen from 0–9, A–Z, and a–z.
	<cr>	No change to level 1 password.
LOGIN_NAME	dd...d	Login name for Level 1 password; up to 11 characters chosen from 0–9 and A–Z.
NPW2	xxxx	New level 2 login password; 4–16 characters chosen from 0–9, A–Z, and a–z
	<cr>	No change to level 1 password.
LOGIN_NAME	dd...d	Login name for Level 2 password; up to 11 characters chosen from 0–9 and A–Z.
LAPW	nn	LAPW password number to change (0–99).
	X nn	X nn removes password nn.
	<cr>	End changes to LAPW passwords.
PWnn	dd...d	New password for LAPW password number nn; 4–16 characters chosen from 0–9, A–Z, and a–z.
	<cr>	No changes to password nn.
LOGIN_NAME	dd...d	Login name for password nn; up to 11 characters chosen from 0–9 and A–Z.
- OVLA	(XALL) xx xx xx...xx ALL	Add these overlays to the list accesses by password PWnn. Xnn removes the overlay.

Table 31
LD 17: Define LAPW options and passwords. (cont'd.)

Prompt	Response	Description
- CUST	(XALL)	(No customers), customer number, or all customers
	0–99	Range for Large System and CS 1000Esystem.
	0-31	Range for Small System, Call Server 1000S system, and Media Gateway 1000B, and Media Gateway 1000T.
	ALL	All customers
- TEN	xxx xxx...xxx, ALL (XALL)	Tenant list for the above customer for password access. XALL removes tenant access for this password.
HOST	(NO) YES	Host mode
- OPT		Password Options
	(CFPA) CFPD	Changes to all LD 17 prompts (Allowed) Denied
	(LLCD) LLCA	Line Load Control commands (Denied) Allowed
	(FORCD) FORCA	(Deny) Allow user to invoke the FORCe command (requires that Multi-User Login be equipped).
	(MOND) MONA	(Deny) Allow user to invoke the MONitor command (requires that Multi-User Login be equipped).
	(PROD) PROA	Print Only Class of Service (Denied) Allowed
	(PSCA) PSCD	Printing Speed Call lists (Allowed) Denied
LAPW	<cr>	Stop defining passwords
- FLTH	0–(3)–7	Failed logon attempt threshold
- LOCK	0–(60)–270	Lockout time in minutes
- AUDT	(NO) YES	Audit Trail (denied) allowed.
- -SIZE	(50) –1500	Word size stored in the Audit Trail buffer
-INIT	(NO) YES	Reset ports locked out during manual INIT.

Each user can change their own LAPW password. Table 32 "LD 17: Change an LAPW password (user must log in using the current LAPW)." (page 118)lists the responses you must enter to change your LAPW password.

Table 32
LD 17: Change an LAPW password (user must log in using the current LAPW).

Prompt	Response	Description
REQ	CHG	Change
PWD2	<cr>	Level 2 master password

Table 32
LD 17: Change an LAPW password (user must log in using the current LAPW). (cont'd.)

Prompt	Response	Description
- LPWD	aaaa	Login Password for LAPW user
- NLPW	xx...x	New login password for LAPW user

You can display the LAPW password options on the active TTY. Table 33 "LD 22: Print options available for LAPW passwords (administrator)." (page 119)lists the LAPW password print options available for administrators.

Table 33
LD 22: Print options available for LAPW passwords (administrator).

Prompt	Response	Description
REQ	PRT	Print
TYPE	PWD	Password
PWD2	xxxx	Level 2 master password
FLTH	x	Failed logon attempt threshold
LOCK	xx	Lock-out time in minutes
AUDT	aaa	Audit Trail allowed (denied)
SIZE	xxxx	Word size stored in the Audit Trail buffer
INIT	aaa	Reset ports locked out during manual INIT
PWD1	xxxx	Level 1 master password
LOGIN_NAME	aaaa...	Login name for Level 1 master password
PWD2	xxxx	Level 2 master password
LOGIN_NAME	aaaa...	Login name for Level 2 master password
PWxx	aaaaaa...	LAPW password number and password
LOGIN_NAME	aaaa...	Login name for LAPW password
OVLA	xx xx xx...	Overlays accessible by this password
CUST	xx TEN xx	Customer number and tenant number accessible
HOST No	xx	Host mode
OPT	aaaaÉ	Password options allowed

The print options available for LAPW vary depending on the permissions of the user who is logged on. Available options are displayed on the active TTY. Table 34 "LD 22: Print options for LAPW password (user)." (page 120)lists the LAPW password print options available for users.

Table 34
LD 22: Print options for LAPW password (user).

Prompt	Response	Comment
REQ	PRT	Print
TYPE	PWD	Password
PWD2	<cr>	Administrator's password
PWxx	aaaaaaÉ	LAPW password number and password
LOGIN_NAME	aaaaÉ	Login name for LAPW password
OVLA	xx xx xx É	Overlays accessible by this password
CUST	xx TEN xx	Customer number and tenant numbers accessible
Host	No	Host mode
OPT	aaaaÉ	Password options allowed
PWxx	aaaaaa...	LAPW password number and password

To display the contents of the Audit Trail buffer, you must log in using PWD1 or PWD2. Table 34 "LD 22: Print options for LAPW password (user)." (page 120)lists the responses you must enter to display the contents of the Audit Trail buffer.

Table 35
LD 22: Print contents of Audit Trail buffer (allowed if using PWD1 or PWD2).

Prompt	Response	Comment
REQ	PRT	Print
TYPE	AUDT	Audit Trail

Feature operation

The normal login sequence is as follows:

LOGI ADMIN1 <cr>

PASS? <pwd1>

>

Enter only one space between LOGI and the login name. If you enter more than one space, the system ignores the login name.

For information on setting and changing LAPW passwords after login, see "Feature implementation" (page 116).

Meridian Mail Voice Mailbox Administration

Use the Meridian Mail Voice Mailbox Administration (VMBA) feature to administer and maintain the Meridian Mail Voice Mailbox application. This feature streamlines the process of implementing and maintaining Voice Mailboxes (VMBs).

Use VMBA to do the following:

- Access the Voice Mailbox Application through LDs 10 and 11 rather than through a separate terminal.
- View application and mailbox statistics to help ensure the integrity of the application.
- Synchronize the system and Meridian Mail databases using special audit and upload functions.
  - The audit function helps ensure that name data stored on the system is synchronized with name data stored on Meridian Mail. You can run the audit manually or configure the system to automatically run it at set intervals.
  - For sites that want to implement VMBA and already have VMBs configured on Meridian Mail, use the VMBA upload command to create or update the system VMB database from the existing Meridian Mail VMB database. Using the upload command can significantly reduce the time required to implement VMBA.

Access to Meridian Mail VMB administration functions is still available using the Meridian Mail administration console. However, to prevent database inconsistencies, use the system for VMB administration when VMBA is equipped.

Telephone types supported include the Meridian Modular telephones, M2317, M2000, M3000, and analog (500/2500-type) telephones.

For a complete description of VMBA, refer to *Features and Services (NN43001-106)*.

MSDL Serial Data Interface

A Serial Data Interface (SDI) extends the I/O capability of the Multi-purpose Serial Data Link (MSDL) card by providing an asynchronous serial data interface. SDI is composed of software components that reside on the system and the MSDL card.

The MSDL SDI supports three asynchronous serial data applications:

- TTY
- PRT
- STA

For more information about STA, see “Single Terminal Access” (page 151).

In addition to the data transmission parameters supported for an MSDL SDI port, you can specify functions for the port, including the following:

- Autobauding
- Line mode editing (LME) for VT220 terminals
- XON/XOFF handling for printer interfaces
- Character screening to avoid system lockup on invalid characters
- Smart and dumb modem support
- DTR/CTS detection
- Serial Data Application autorecovery

The following capabilities are available on the MSDL SDI:

- Interfaces to TTYs, printers, modems, and CRTs
- High Speed Link (HSL) for ACD
- Auxiliary Processor Link (APL) for ACD
- ACD Package C displays and reports
- CDR TTY
- Maintenance TTY
- Bug and error messages
- LD 2 and traffic measurements
- Filtered alarms
- Data administration

Functions

This section describes the major functions provided by the MSDL SDI.

Autobauding

Enable Autobauding if you want the MSDL card to detect the baud rate of data transmission (from 300 to 38,400 bps) and report it to the system; the system sends the baud rate to the SDI port. Autobauding helps eliminate the problem of baud rate mismatches and thereby reduces the risk of a port lockout.

Line Mode Editing

Enable Line Mode Editing (LME) to allow an entire line to be entered before it is transmitted to the system. If Line Mode Editing is not enabled, each character is transmitted as soon as it is typed. This function is only supported for VT220-type terminals running EM200 emulation mode.

XON/XOFF handling

Use XON and XOFF to control data output from an MSDL SDI data port. XOFF suspends data output; XON resumes data output. The MSDL card stores up to 500 characters in its buffer; when this capacity is exceeded, newer data overwrites the oldest data.

Character screening

Normal communication includes input and output character transfer, with the SDI application transmitting all characters received from the system to the connected device. You can configure the MSDL SDI to check for invalid entries before transmitting characters to the system. Valid characters include the following:

- alphabetic characters: A–Z, a–z
- numeric characters: 0–9
- all hexadecimal characters in the range H.20 through H.7E, plus Carriage Return, Line Feed, <Ctrl-D>, <Ctrl-P>, and <Ctrl-T>. Backspace and <Ctrl-R> are valid if LME is turned on.

Modem support

The SDI application automatically detects if the modem for the SDI port is currently connected and operational. If a modem is not detected, no data is sent to or received from the modem. This prevents smart modems from echoing characters received from the system.

DTR/CTS detection

When the MSDL SDI is configured as Data Communications Equipment (DCE), it monitors the DTR signal. When it is configured as Data Terminal Equipment (DTE), it monitors the CTS signal. If a signal is low when the port is enabled, the system sends a message indicating the problem and the MSDL SDI does not release output. When the signal returns to a higher level, another message appears and output resumes.

Serial Data Application autorecovery

The MSDL SDI provides an autorecovery mechanism for Serial Data Applications. If the system disables the MSDL card or MSDL SDI port while a Serial Data Application (such as HSL or APL) is active, the system attempts to restart the application when the MSDL card or MSDL SDI port is re-enabled. However, if you manually disable the MSDL card or the MSDL SDI port while a Serial Data Application is active, the system does not attempt to restart the application when the MSDL card and MSDL SDI port are re-enabled.

Function applicability to serial data applications

The types of serial data applications and users running on the SDI port determine the specific functions available to the port, as shown in Table 36 "Available port functions" (page 124).

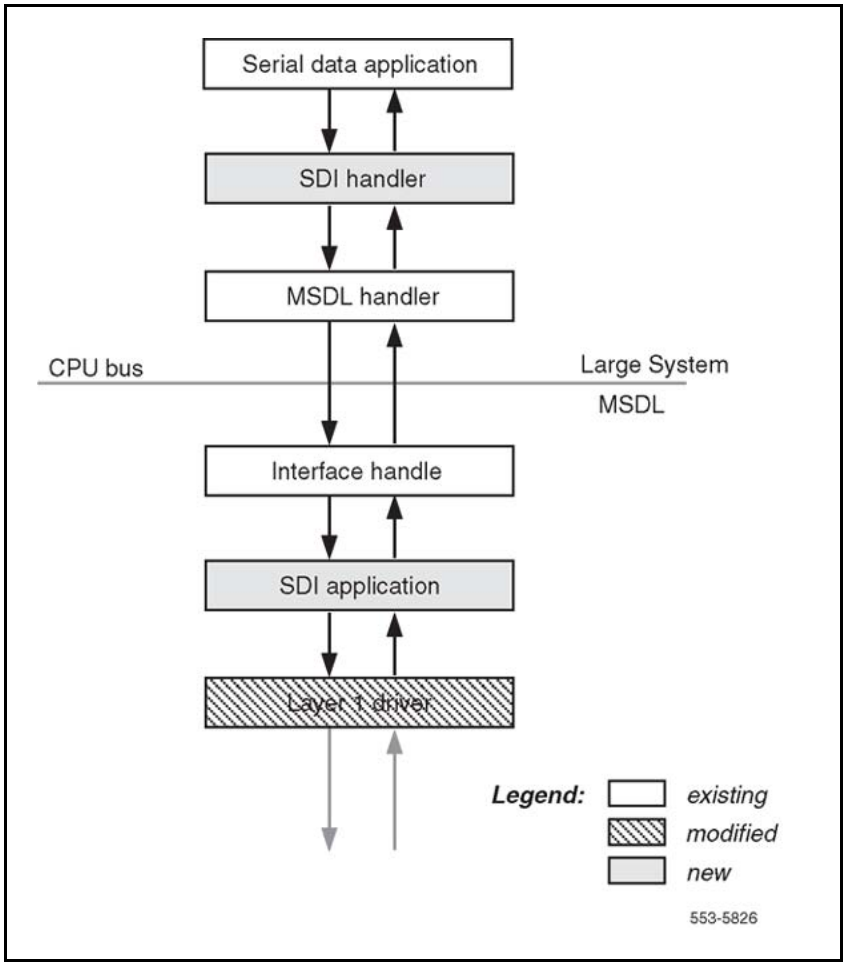
Table 36
Available port functions

	Autobaud	Modem Support	XON/XOFF Handling	Line Mode Editing	Character Screening
Maintenance TTY (User types of BUG, CSC, MTC, SCH, FIL)	Yes	Yes	Yes	Yes	Yes
Application TTY (User types of TRF, CTY, BGD)	Yes	Yes	Yes	Yes	Yes
Application Link (User types of ACD, APL, HSL, PMS)	No	Yes	No	No	No
System Monitor XSM	No	No	No	No	No
PRT	No	Yes	Yes	No	No

The port functions do not apply to a system power port (an SDI defined with XSM = YES and USER = MTC).

Figure 14 "MSDL SDI software components" (page 125) illustrates the software components that comprise the MSDL SDI.

Figure 14
MSDL SDI software components



Operating parameters

SDI ports on the MSDL are configured with full-duplex communication. The data transmission parameters are listed below, with default values in parentheses. Use LD 17 to change the values.

- Cable connection: (RS–232), RS–422
- Baud rate: 300, 600, (1200), 2400, 4800, 9600, 19 200, or 38 400 bps
- Number of data bits: 7, (8)
- Number of stop bits: (1), 1.5, 2
- Parity: Odd, Even, (None)
- Transmission mode: If the device is a TTY, the default is DCE; if the device is a PRT, the default is DTE.

If you specify 8 data bits specified, the system transmits the high order bit as 1. If the terminal is not equipped to handle this data it displays the characters improperly. In Line Mode Editing (LME), the MSDL provides 8-bit output that displays properly on the terminal.

To abort a self-test running on an MSDL port, enter "END". You cannot abort a self-test by entering four asterisks (****).

If you change the configuration for an MSDL port (for instance, if you change the baud rate, or activate autobaud support), the change does not take effect until the port is disabled and re-enabled, either manually through a maintenance overlay, or through a manual initialization.

The MSDL SDI sends output only if the DTR (for DCE) or CTS (for DTE) signal is high.

You cannot configure breakpoints from an MSDL SDI.

Operational characteristics for a Large System include the following:

- The task must be running for the normal functioning of the MSDL SDI ports.
- The Line Mode Edit (LME) function replaces the lon/LON and lof/LOF commands.
- The Flow Control (FCL) function replaces the FLOW and BCST prompts.

An MSDL SDI TTY cannot be used as a dumb device for connecting to SLIP for file transfers.

Feature interactions

You can connect the MSDL SDI port to an auxiliary port. If the auxiliary port does not use the MSDL SDI functions (such as autobauding and line mode editing), then the operation of the port is unaffected. However, if the auxiliary port uses any of the MSDL SDI functions, modification of other applications can be necessary.

If you use an MSDL SDI card with a modem that is configured for the Property Management System Interface (PMSI) link, the MSDL SDI driver can transmit or receive a message only when the modem is connected. The system periodically polls PMS; if the modem is without power or is not connected, the polling message is not delivered, and the system assumes that the link is not responding.

Feature packaging

MSDL SDI requires the following packages:

- Multi-purpose Serial Data Link (MSDL) package 222
- MSDL Serial Data Interface (MSDL SDI) package 227

Feature implementation

The MSDL SDI is available for all machine types except the Small System. It coexists on the MSDL with the CPSI, DCHI, MSPS, SDI, SDI2, SDI4, and XSDI cards.

The following limitations apply:

- Only port 0 on the MSDL can be configured as an SDI asynchronous port.
- All MSDL SDI functions do not apply to all Serial Data Applications. For example, autobauding is not supported for printers.
- Autobauding only detects the baud rate; it does not detect parity, stop bits, and number of data bits.
- Users cannot configure breakpoints from an MSDL SDI port.
- In a few cases, sysload and init messages may not print depending on the state of the MSDL and the information stored in the MSDL EEPROM (Electrically Erasable Programmable Read-Only Memory).
- If an MSDL SDI port is disabled during a manual init or a post-sysload init, init messages do not print on the port before it is brought up.

Response to the following prompts in LD 17 activates the MSDL SDI.

Table 37
LD 17: Configure MSDL SDI.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action Device And Number
ADAN	NEW CHG OUT TTY < 0–15>	Teletype <device number>
	PRT <0–15>	Printer <device number>
CTYP	MSDL	Card type = Multi-purpose Serial Data Link
GRP	0–7	Network group numbers (only prompted for a Large System)
DNUM	0–15	Device number; autoprinted by system

Table 37
LD 17: Configure MSDL SDI. (cont'd.)

Prompt	Response	Description
PORT	0	Port number on MSDL card; autoprinted by system if CTYP=MSDL
DES	aa...aa	Port designator; 1–16 characters, in the range of 0–9 and A–Z and some special characters (not including spaces, *, $, or #)
	Xaa	Precede entry with X to delete an existing name before trying to enter a new one
BPS	300 600 (1200) 2400 4800 9600 19200 38400	Baud rate
PRTY	(NONE) ODD EVEN	Parity
STOP	(1) 1.5 2	Stop bits
BITL	7 (8)	Data bit length
PARM	aaa bbb	Port functions. Where aaa = R232 or R422 and bbb = DTE or DCE. Default is: R232 DCE for TTY, R232 DTE for PRT
FUNC		MSDL card function. Precede with an X to remove a function (for example, XLME)
	LME	Line mode editing
	ABD	Autobaud
	FCL	Flow control (XON/XOFF)
	SCN	Character screening
	MOD	Model support
USER		User types. When ADAN = HST, users may be BUG, MCT, MTC, or SCH or TRF.
	ACD	Automatic Call Distribution printer for reports
	APL	Auxiliary Processor Link for IVMS
	BGD	Background Terminal
	BUG	Software error
	CSC	Customer Service Changes
	CTY	CDR TTY port to output CDR records
	HSL	ACD/D High-Speed AUX link
	MTC	Maintenance
	NOO	No Overlay allowed
	PMS	Property Management System interface

Table 37
LD 17: Configure MSDL SDI. (cont'd.)

Prompt	Response	Description
	SCH	Service Change
	TRF	Traffic

Sample configurations

This section includes sample configurations for five situations:

- an existing terminal to be used for regular maintenance functions
- an MSDL SDI with a remote maintenance terminal
- an MSDL SDI with a VT220 terminal and Line Mode Editing
- a printer port connected to a smart printer
- a special link

Sample 1: An existing terminal (such as a VT100) to be used for regular maintenance functions

Table 38
LD 17: Prompts and responses for Sample 1.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action Device And Number
ADAN	NEW STA 0–15	Assign an ID # to the STA application (up to 16 are allowed)
TTY	0–15	The number of the predefined MSDL SDI TTY
CTYP	MDSL	Multi-purpose Serial Data Link card type
GRP	0–7	Network group number
DNUM	0–15	Device number for I/O ports (same value as for TTY above)
ADMIN_PORT	0	STA Admin terminal port # (must be 0)
LANGUAGE	ENGLISH	Language for STA; supports only ENGLISH
DES	aaa...a	For example, Maint_TTY; up to 16-character designation; no blanks, *, $, or !
BPS	9600	Baud rate (default 4800)
PARY	none	Parity type
STOP	1	Number of stop bits
BITL	7	Data bit length
PARM	RS232 DCE	Interface and transmission mode

Table 38
LD 17: Prompts and responses for Sample 1. (cont'd.)

Prompt	Response	Description
FUNC	<CR>	Initially, no new functions
USER	MTC SCH BUG	Maintenance, service change, and software error messages
XSM	no	SDI port for the System Monitor
TTYLOG	<CR>	
ADAN DATA SAVED		

Note 1: Ensure that the terminal is configured to the same parameters: 9600 baud, no parity, 7 data bits, 1 stop bit.

Note 2: Because the SDI port is DCE, the terminal is DTE.

Note 3: If using an extension cable, verify that it carries the main RS232 leads, such as DTR.

Note 4: Possible functions for this terminal include ABD (autobauding) and SCR (screen out unrecognized characters).

Sample 2: An MSDL SDI with a remote maintenance terminal (or a PC running VT100 emulation) through a modem

Table 39
LD 17: Prompts and responses for Sample 2.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action Device And Number
ADAN	NEW STA 0–15	Assign an ID # to the STA application (up to 16 are allowed)
TTY	0–15	The number of the predefined MSDL SDI TTY
CTYP	MSDL	MSDL card type
GRP	0–7	Network group number
DNUM	0–15	Device number for I/O ports (same value as for TTY above)
ADMIN_PORT	0	STA Admin terminal port # (must be 0)
LANGUAGE	ENGLISH	Language for STA; supports only ENGLISH
DES	aaa...a	For example, Typical_Modem; up to 16-character designation; no blanks, *, $, or !
BPS	2400	Baud rate (default 4800)
PARY	none	Parity type
STOP	1	Number of stop bits

Table 39
LD 17: Prompts and responses for Sample 2. (cont'd.)

Prompt	Response	Description
BITL	7	Data bit length
PARM	RS232 DTE	Interface and transmission mode
FUNC	ABD MOD	Autobauding, modem support
USER	MTC SCH BUG	Maintenance, service change, and software error messages
XSM	no	SDI port for the System Monitor
TTYLOG	<cr>	
ADAN DATA SAVED		

Sample 3: An MSDL SDI with a VT220 terminal and Line Mode Editing

Table 40
LD 17: Prompts and responses for Sample 3.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action device and number
ADAN	NEW STA 0–15	Assign an ID # to the STA application (up to 16 are allowed)
TTY	0–15	The number of the predefined MSDL SDI TTY
CTYP	MSDL	Multi-purpose Serial Data Link card type
GRP	0–7	Network group number for Large Systems
DNUM	0–15	Device number for I/O ports (same value as for TTY above)
ADMIN_PORT	0	STA Admin terminal port # (must be 0)
LANGUAGE	ENGLISH	Language for STA; supports only ENGLISH
DES	aaa...a	For example, Super_Terminal; up to 16-character designation; no blanks, *, $, or !
BPS	19200	Baud rate (default 4800)
PARY	none	Parity type
STOP	1	Number of stop bits
BITL	8	Data bit length; must be 8
PARM	RS232 DCE	Interface and transmission mode
FUNC	ABD FCL LME	Autobauding, XON/XOFF, Line Mode Editing

Table 40
LD 17: Prompts and responses for Sample 3. (cont'd.)

Prompt	Response	Description
USER	MTC SCH BUG	Maintenance, service change, and software error messages
XSM	no	SDI port for the System Monitor
TTYLOG	<CR>	
ADAN DATA SAVED		

Sample 4: A printer port connected to a smart printer

Table 41
LD 17: Prompts and responses for Sample 4.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action device and number
ADAN	NEW/CHG STA 0–15	Assign an ID # to the STA application (up to 16 are allowed)
TTY	0–15	The number of the predefined MSDL SDI TTY
CTYP	MSDL	Multi-purpose Serial Data Link card type
GRP	0–7	Network group number
DNUM	0–15	Device number for I/O ports (same value as for TTY above)
ADMIN_PORT	0	STA Admin terminal port # (must be 0)
LANGUAGE	ENGLISH	Language for STA; supports only ENGLISH
DES	aaa...a	For example, TRF_Printer; up to 16-character designation; no blanks, *, $, or !
BPS	9600	Baud rate (default 4800)
PARY	none	Parity type
STOP	1	Number of stop bits
BITL	7	Data bit length
PARM	<cr>	Uses system default of RS232 DTE
FUNC	FCL	XOFF/XON support
USER	TRF	Traffic
XSM	no	SDI port for the System Monitor
TTYLOG	<cr>	
ADAN DATA SAVED		

Sample 5: A special link

Table 42
LD 17: Prompts and responses for Sample 5.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action device and number
ADAN	NEW/CHG STA 0–15	Assign an ID # to the STA application (up to 16 are allowed).
TTY	0–15	The number of the predefined MSDL SDI TTY
CTYP	MSDL	Multi-purpose Serial Data Link card type
GRP	0–7	Network group number for Large Systems
DNUM	0–15	Device number for I/O ports (same value as for TTY above)
ADMIN_PORT	0	STA Admin terminal port # (must be 0)
LANGUAGE	ENGLISH	Language for STA; supports only ENGLISH
DES	aaa...a	For example, High_Speed_Link; up to 16-character designation; no blanks, *, $, or !
BPS	9600	Baud rate (default 4800)
PARY	none	Parity type
STOP	1	Number of stop bits
BITL	8	Data bit length
PARM	RS232 DCE	Interface and transmission mode
FUNC	<CR>	Only valid entry is MOD for Modem
USER	HSL	PMS, APL, and ACD are other valid special links
XSM	no	SDI port for the System Monitor
TTYLOG	<CR>	
ADAN DATA SAVED		

Feature operation

Initialization

The SDI application that resides on the MSDL and the individual MSDL SDI port must be initialized. Global initialization occurs after the application is downloaded to the MSDL. The system issues a command to the MSDL to enable the application, creating different tasks for the application. Each task initializes any necessary private data and creates an input queue. The SDI application also provides maintenance socket identification to MSDL maintenance and the system Interface Handler.

Port initialization occurs when the system software requests that an SDI port be enabled. The SDI application registers with the system Interface Handler and the Layer 1 Driver. The EEPROM stores SDI parameters such as baud rate, parity, number of stop bits, number of data bits, DTE or DCE, RS-232 or RS-422, and SDI or other asynchronous applications. These parameters are used for printing sysload messages when the MSDL is resetting.

If there is not enough memory during initialization to allocate local data structures or to register with the system interface, or if the Layer 1 Driver fails for any reason, the system is notified.

Enable Not Ready (ENBL NRDY)

An enabled MSDL SDI port can become Not Ready for any of the circumstances listed below. The effect on the system depends on the cause of the Not Ready state.

- The DTR/CTS signal is down, or, if MOD is configured, the modem call has been disconnected.
- A port is autobauding. When autobauding is in progress, output is sent at 9600 baud until the system detects the actual baud rate.
- A port is configured for LME and a terminal verification test is in progress. The system sends no output.
- The function MOD is specified for the port. No call has been established. The system sends no output.

Autobauding

Users should enter Carriage Returns (H.0D) to trigger autobauding. Autobauding only determines the baud rate; a service change is required to specify parity, number of stop bits, and number of data bits.

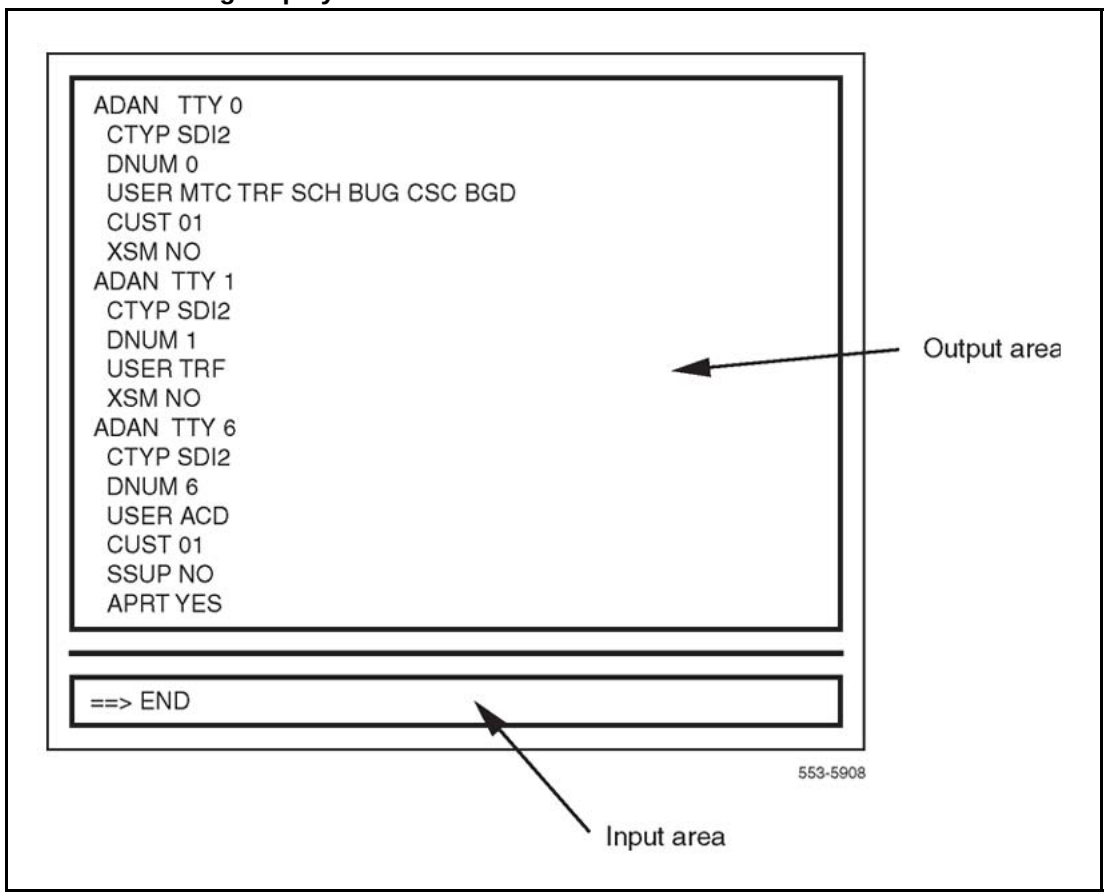
After an SDI port has been enabled (and, with a modem connection, connected), the autobauding process starts. If the modem connection is dropped and then reestablished (or the terminal is disconnected, then reactivated) the port restarts the autobauding process, and presents the detected baud rate to the user.

Line Mode Editing (LME)

The SDI application buffers up to 80 input characters per line. Backspacing is allowed with either <Ctrl-H> (H.8) or Delete (H.7F). The user sends a line in a block by entering a Carriage Return or a Line Feed (see Figure 15 "Line Mode Editing display" (page 135).)

If an MSDL port has line mode editing turned on, the high-order bit of an 8-bit character sent by the system is cleared, whether or not the Multi-Language TTY I/O package 211 is equipped.

Figure 15
Line Mode Editing display



XON/XOFF handling

Use this function if the SDI port is connected to a printer that cannot keep up with the system output. The printer can use XOFF and XON to adjust the pace of the output. The XON character is <Ctrl-Q> (H.13); the XOFF character is <Ctrl-S> (H.11).

An XOFF suspension cannot exceed one minute. After one minute, SDI empties the buffers, resumes operation, and sends a message that data has been lost, if applicable.

Abnormal operation

If the MSDL is in the Reset state (with only boot code running), sysload messages print using the parameters stored in the EEPROM. If the EEPROM has not been configured, sysload messages print on port 0 with

default parameters (baud rate=1200, data bits=8, stop bit=1, parity=NONE, RS232, DCE). If the jumper setting on the card is not configured for an RS-232 interface, no printing occurs.

If the MSDL is enabled (with base code running), SDI ports send sysload messages if the SDI application has also been enabled; otherwise, no messages print.

If there is not enough memory to allocate local data structures during SDI port initialization, or if registration with the system Interface Handler or Layer 1 Driver fails, the system is notified.

If the MSDL SDI application needs to be downloaded to the MSDL card during initialization, the connected device does not obtain all init messages generated.

Whenever the Layer 1 Driver detects an input parity or framing error, it discards the input character and does not notify the SDI application.

Multi-User Login

Multi-User Login (MULTI_USER) package 242 enables up to five users to log in, load, and execute overlays simultaneously. These five users are in addition to an attendant console or maintenance terminal. The multi-user capability increases efficiency by allowing several technicians to perform tasks at the same time. To facilitate this operating environment, Multi-User Login includes the following:

- Database conflict prevention
- Additional user commands
- TTY log files
- TTY directed I/O

With multiple overlays operating concurrently, there is the potential for a database conflict if two or more overlays attempt to modify the same data structure. Multi-User Login software prevents such conflicts. When a user requests that an overlay be loaded, the software determines if it could pose a potential conflict with an overlay that is already executing. If no conflict exists, the requested overlay is loaded. If a conflict does exist, the system issues the following message:

```
OVL429-OVERLAY CONFLICT
```

The user can try again later or try to load a different overlay.

For Release 7.0 and greater, the overlay conflict resolution check is relaxed to allow Multi-User overlays to operate concurrently with LD 43, if only the database backup is performed on the Overlay. For example, backup to removable storage media, CCBR or GR backup.

The following Multi-User Login commands are available:

- Communicate with other users
- Determine who is logged in to the system
- Halt and resume background and midnight routines
- Initiate and terminate terminal monitoring
- Change printer output assignment

See "User commands" (page 140) for instructions on how to use these commands.

With Multi-User Login active, the system shifts TTY output to direct I/O mode, so that output to the TTY only appears on the specific terminal for which it is intended.

The TTYLOG prompt in LD 17 creates a log file of the specified size for the TTY.

LD 22 supports viewing (printing) of a TTY log file. See "Feature implementation" (page 139) for specific instructions.

Number of users

The number of users allowed to log in at the same time is five. Multi-User capability is also extended to LD 2 and LD 87.

Element Manager

Multi-User Login applies to Element Manager. Multi-User Login enables as many users to login to Element Manager as there are pseudo-teletype terminals (PTYs) configured on the system. However, only four users can simultaneously make changes.

Subscriber Manager

The maximum number of simultaneous users supported when performing the same work flow is 10.

Operating parameters

Maintenance routines cannot run while midnight or background routines are running. An attempt to load a maintenance routine suspends or terminates the midnight or background routines first (except for LD 44, Audit, which can run at all times).

To prevent unnecessary database conflicts, the following rules govern the concurrent execution of multiple overlays:

- Only one maintenance overlay can run at a time.
- Only one service change overlay can run at a time, except for LD 10/11.
- Only one copy of LD 32, LD 44, and LD 80 can run at a time, but each copy can run with other overlays.
- Multiple copies of LD 10, LD 11, LD 20, LD 21, and LD 22 can run at a time.

Valid overlay combinations are shown in Table 43 "Sample overlay combinations" (page 138).

Feature interactions

Nortel recommends that Limited Access to Overlays (LAPW) package 164, which provides expanded password support, be activated on a system using Multi-User Login. With LAPW, you can assign up to 100 user passwords, and use password assignment to delineate users' access to specific overlays. This approach creates a more secure user environment by limiting user access and providing audit trails of user activity. See "Limited Access to Overlays" (page 113) for more information.

Feature packaging

This feature requires Multi-User Login (MULTI_USER) package 242. To print the TTY log files requires that History File (HIST) package 55 be active.

Table 43
Sample overlay combinations

User 1	User 2	User 3	Background
Set Admin (LD 10/11)	Set Admin (LD 10/11)	Set Admin (LD 10/11)	Maintenance Login/Midnight routines
Set Admin (LD 10/11)	Set Admin (LD 10/11)	Print (LD 20/21/2220/21/22)	Maintenance Login/Midnight routines
Set Admin (LD 10/11)	Print (LD 20/21/22)	Print (LD 20/21/22)	Maintenance Login/Midnight routines
Set Admin (LD 10/11)	Set Admin (LD 10/11)	Maintenance (LD 32, 37)	Audit routines (LD 44)
Note: Attendant Administration (AA) cannot run with Set Admin (LD 10/11).			

Table 43
Sample overlay combinations (cont'd.)

User 1	User 2	User 3	Background
Set Admin (LD 10/11)	Print (LD 20/21/22)	Maintenance (LD 32, 37)	Audit routines (LD 44)
Print (LD 20/21/22)	Print (LD 20/21/22)	Not in use	Maintenance Login/AA/Midnight routines
Print (LD 20/21/22)	Print (LD 20/21/22)	Print (LD 20/21/22)	Maintenance Login/AA/Midnight routines
Note: Attendant Administration (AA) cannot run with Set Admin (LD 10/11).			

Feature implementation

Use LD 17 to activate Multi-User Login.

Table 44
LD 17: Activate Multi-User Login.

Prompt	Response	Description
REQ	CHG	Change
TYPE:	OVLY	Overlay gateway
SID	<cr>	System ID number
MULTI_USER	(OFF) ON	(Deactivate) Activate multi-user login

Use LD 17 to allow or disallow the FORCE and MONITOR commands.

Table 45
LD 17: Allow or disallow the FORC and MON commands.

Prompt	Response	Description
REQ	CHG	Change
TYPE:	PWD	Password
PWD2	aa...aa	The current level 2 password
LAPW	nn	LAPW password number
PWnn	ff...ff <cr>	Change LAPW password nn Do not change password
OPT	(FORCD) FORCA	(Deny) Allow user to invoke FORC command
	(MOND) MONA	(Deny) Allow user to invoke MON command

Use LD 22 to print the values of TTYLOG and MULTI_USER

Table 46
LD 22: Print TTYLOG and MULTI_USER values.

Prompt	Response	Description
REQ	PRT	Print
TYPE	ADAN TTY n	Print TTYLOG value if USER = MTC, SCH, TRF, BUG, or FIL
VHST	(HST)	View the system History File
	TTYLOG n	View the log file for TTY port n
	TRF	View the system Traffic Log File
TYPE	PKG 242	Prints MULTI_USER values

Feature operation

Initiating a Multi-User Login session is the same as initiating a single-user session. The normal login process is followed by issuing the LD xx command to load an overlay. If other overlays are running, a message appears identifying the other terminal IDs, login names, and overlay numbers.

System software checks to ensure that the requested overlay can run concurrently with the other overlays. If it cannot, message OVL429 identifies an overlay conflict. (An overlay conflict arises when two or more overlays modify the same data structure concurrently, which may cause data corruption.) If there is no conflict, the system loads the overlay and invites the user to initiate tasks.

User commands

A user can issue the commands listed and described in Table 47 "User commands" (page 140) at the > prompt (after login but with no overlay executing), or from within an overlay. To issue a command from within an overlay, precede the command with an exclamation point (!).

For example, to issue the WHO command from within an overlay, type:

```
!WHO
```

Table 47
User commands

Command	Description
WHO	Display user name, port ID, and overlay loaded for each logged-in terminal, as well as the user's MON and SPRT commands (see below).

Table 47
User commands (cont'd.)

Command	Description
SEND xx	Send a message to logged-in terminal xx. When the system responds with a "SEND MSG:" prompt, enter the message text yy...yy (up to 80 characters). The text of a message is considered private and therefore is not written to any log file.
SEND ALL	Send a message to all logged-in terminals. When the system responds with a "SEND MSG:" prompt, enter the message text yy...yy (up to 80 characters). The text of a message is considered private and therefore is not written to any log file.
SEND OFF	Prevent messages sent by other terminals from appearing at the user's terminal.
SEND ON	Enable messages sent by other terminals to appear at the user's terminal.
FORC xx	Force terminal xx to log off (the requesting user must log in with LAPW or a level 2 password).
HALT	Stop background and midnight routines during a login session.
HALT OFF	Resume halted background and midnight routines.
MON xx	Initiate monitoring for terminal xx (the requesting user must log in with LAPW or a level 2 password). The monitored terminal receives a message at the beginning and end of the monitored period.
MON OFF	Turn off the monitor function.
SPRT xx	Assign printer output to port xx.
SPRT OFF	Reset printer output assignment.

Set-Based Administration

Set-Based Administration provides three levels of set-based data administration access:

- You can use Administration Access to make changes to any supported telephones within the same customer location. You can perform any of the following tasks through an administration/maintenance telephone (M2008, M2016, M2216, M2616 with display):
  - Change the data associated with specific telephone-related features (such as Hunting, External Hunting, Call Forward No Answer, External Call Forward No Answer, Call Forward, Busy

Forward Status, Voice Call, Dial Intercom Group, Group Call, Ringing Number Pickup Group, Speed Call, System Speed Call, and Hot Line).

— Add or change the Calling Party Name Display (CPND) names associated with existing DNs.

— Change system date and time.

— Change toll restrictions of any telephone.

– Determine Directory Number-Terminal Number correspondence.

- Installer Access allows an installer to perform any of the following tasks to a telephone from which the installer is logged in to:

  — Change the data associated with specific telephone-related features.

  — Add or change the Calling Party Name Display names associated with the DN on that telephone.

  — Change system data and time.

  — Change toll restriction for that telephone.

- User Installation allows a user to add or change the user's own CPND when logging in through the user's own telephone.

Administrator and Installer Access are invoked by dialing the Administrator or Installer Flexible Feature Code (FFC) followed by the Administrator or Installed password. The passwords are defined on a system basis. User Access is activated by dialing the Set-Based Administration User FFC followed by the Station Control Password of the user's telephone.

As well as displaying useful information on the telephone's display, sound cues are employed for the benefit of users logged in to Set-Based Administration (SBA) on telephones without displays. Four seconds of overflow tone indicates the user made an error, while four seconds of special dial tone indicates a data change was successfully completed.

The multi-language capability of this feature supports all languages currently supported on the Small System. These languages are English, German Spanish, Swedish, Canadian and Parisian French, Dutch, Italian Danish Portuguese, and Norwegian. Changing between languages is performed by changing the display language on the Meridian Modular telephone using the telephone's PROGRAM key.

For a Small System, the functionalities are grouped under the following two tasks on the **Main Menu**, under administration access:

- Administration: provides a grouping of trunk-related options.
- Installation options: provides the same functions as before; however, it is moved to a new location on the **Main Menu**.

Since these two capabilities are only available in the Small System, they are not displayed on the **Main Menu** for other system types.

Operating parameters

With the exception of CPND, features cannot be added to or deleted from a telephone using this feature.

The CPND name change enhancement to Set-Based Administration is not supported using non-display telephones, due to the complexity of operation without visual feedback.

If the user has the ability to see the data, the data can be changed.

With the exception of CPND support, the Meridian Mail subsystem integration is not supported. Meridian Mail mailbox changes cannot be performed by means of Set-Based Administration.

Network login is not supported; a telephone can only login on its home node.

Entry of "*" and "#" in extension numbers is not supported using Set-Based Administration, because these are the keys that the feature uses to control user navigation through the menus.

Access from the system to BRI telephones is not supported.

Set-Based Administration logins cannot be made from Direct Inward System Access (DISA) calls.

Feature interactions

Multi-User Login

The Set-Based Administration Enhancements feature adds additional multi-user login sessions, which will be restricted to Set-Based Administration logins only, over and above the Multi-User Login feature. This prevents the same data from being simultaneously changed by more than one user, whether through TTYs or Set-Based Administration.

Note: The Multi-User Login package is not required for Set-Based Administration.

History file

Set Based-Administration logins and logouts are recorded in the history file. An audit trail of data changes made by means of Set-Based Administration will be recorded in the system history file. The record format is as follows:

ADMINSET (login name)[TN of admin set][time and date stamp]

[CHG:/NEW:](Who's changed)(item changed)(current value->)[new value]

> ***Note:*** Items between [ ] always appear, while items between () appear depending upon the function being performed and/or the configuration options.

Limited Access Passwords (LAPW)

The Set-Based Administration access passwords which are added to LAPW are subject to the same conditions as the overlay access passwords with the following exceptions:

- Set-Based Administration passwords must be numeric.
- There is no maximum number of login attempts for Administrator or Installer sets. Lockout procedures are not used.
- TTY users are not permitted to login using a Set-Based Administration password.
- Administration sets and User sets are not permitted to login using overlay access passwords.
- The total number of LAPW passwords allowed, including overlay access and Set-Based Administration access, is 100.
- The permission and restrictions associated with a Set-Based Administration password used to login to an Administration telephone or Installer telephone remain unchanged throughout the login session. Thus, if a TTY user changes a Set-Based Administration password (in LD 17) while an Administration or Installer telephone is logged in with the same password, the permissions and restrictions associated with the session are not affected. The changes come into effect the next time a user logs in.

Small System Set-Based Installation

The Set-Based Installation functions are not changed by the Set-Based Administration enhancements feature; however, the menu structure is altered.

Maintenance Set

The operation of Maintenance Sets is not affected by the Set-Based Administration enhancements feature; however, a Maintenance telephone becomes an Administration telephone when a user logs in with an Administrator access Set-Based Administration password.

Set Relocation

The operation of Set Relocation is not affected by Set-Based Administration enhancements.

Sets that have been relocated out cannot be administered. Since they no longer have physical TNs, they cannot be selected from an Administration set.

Datadump

Login is not permitted while a datadump is in progress. The result is the overflow tone and the message "LOGIN UNAVAILABLE PLEASE TRY AGAIN LATER" is displayed.

If an attempt is made to load datadump while there are active Set-Based Administration logins, the logins are treated as TTY logins and the situation will be handled by the Multi-User Login feature.

Busy Forward Status

The lamp state of a Busy Forward Status key, which is changed through Set-Based Administration, are updated when the change is completed in the same manner as it is through accessing LD 11 from TTY.

Office Data Administration System (ODAS)

Changes to data blocks made by using Set-Based Administration also cause the ODAS timestamps to be updated.

Remote Call Forward

A telephone may be remote call forwarded while someone is actively logged in to it with a Set-Based Administration login.

Phantom TNs

Set-Based Administration supports making changes to Phantom TNs with the exception of changing Hunt DNs, since Phantom TNs cannot have Hunt DNs.

Network Time Synchronization

Changing the time and date on a master or slave node interacts with the Network Time Synchronization feature, in the same manner as they interact with the attendant change time and date functions.

Feature packaging

Set-Based Administration Set (ADMNSET) package 256 must be used to activate the Set-Based Administration enhancements feature. In addition, the following packages are required:

- Limited Access to Overlays (LAPW) package 164
- Flexible Feature Codes (FFC) package 139

The following software packages are optional and are required only for certain applications:

- M2000 Digital Sets (DSET) package 88
- Calling Party Name Display (CPND) package 95
- Aries Digital Sets (ARIE) package 170
- Automatic Installation (AINS) package 200 (Small System)

Feature implementation

To configure the Set-Based Administration Enhancements feature, complete the following steps:

- Define Set-Based FFCs in LD 57.
- Give Maintenance Allowed (MTA) Class of Service to the Administration telephone.
- In LD 17:
  - Define Set-Based Administration passwords.
  - Enable the Multi-User Login feature.
  - Optionally, define login types for the History File.
  - Optionally, change the maximum number of logins.
  - Optionally, change the maximum number of 500 buffers.

To configure User level access, complete the following additional steps:

- Assign user sets User Level Allowed Access (ULAA) Class of Service in LD 10 and 11.
- Optionally, enable the use of station control passwords in LD 15.
- Optionally, define FFCs on abcd sets.

Table 48
LD 17: Define Set-Based Administration passwords.

Prompt	Response	Description
REQ	CHG	Change
TYPE	PWD	System passwords PWD and Limited Access to Overlay passwords
...		
PWD	YES	Change Passwords options
- PWD2	x..x	Master password. This password is required to change existing PWD1 and PWD2
...		
REQ	CHG	Change
- LAPW	0-99	Limited Access to Overlays Password number
- PWTP	SBA	Set-Based Administration password (see Note 1)
- PWnn	xx.x	Password (must be numeric)
- LOGIN_ NAME	xx.x	Login name for this password, if LAPW login names are enabled in this overlay
- LEVEL	ADMIN, INST	Administrator or installer (see Note 2)
- CUST	xx	Customer number as defined in LD 15.
	(FEAD) FEAA	(Deny) allow Change Set Features (Administrator and installer access)
	(NAMD) NAMA	(Deny) allow Change CPND Names (Administrator & installer access)
	(TADD) TADA	(Deny) allow Set Time and date (Administrator &installer access)
	(TOLD) TOLA	(Deny) allow Change Toll Restrictions (Administrator &installer access)
	(DTD) DTA	(Deny) allow DN-TN Correspondence (Administrator &installer access)
	(TRKD) TRKA	(Deny) allow Change Trunks (Small System Administrator & Installer access)
	(INSD) INSA	(Deny) allow Installation Options (Small System Administrator & Installer access)

Note 1: Only prompted if the ADMINSET package is equipped and the password does not exist.
Note 2: Only prompted for SBA passwords.

Table 49
LD 57: Define Set-Based Administration FFCs.

Prompt	Response	Description
REQ	NEW CHG	Add or change
TYPE	FFC	Flexible Feature Codes (FFC) data block
CUST	xx	Customer number as defined in LD 15.
...		
CODE	ADMIN	Set-Based Administration – Administrator access FFC (see Note)
ADMIN	xxxx	Administrator access FFC (see Note)
CODE	INST	Set-Based Administration – Installer access FFC[1]
INST	xxxx	Installer access FFC
CODE	USER	Set-Based-Administration – User access FFC[1]
USER	xxxx	User access FFC
Note: Only accepted if ADMINSET package is equipped.		

Feature operation

Many operational procedures and set-based menus are available for this feature. For a complete description of the Set-Based Administration feature, refer to *Set-Based Administration (NN43001-603).*

Table 50
LD 11: Assign Maintenance Allowed Class of Service.

Prompt	Response	Comment
REQ:	CHG	Change
TYPE:	2008 2016 2216 2616	Set type with display option equipped
TN	l s c u c u	Terminal number Format for Large System and CS 1000Esystem where l = loop, s = shelf, c = card, and u = unit. Format for Small System, Call Server 1000S system, and Media Gateway 1000B, and Media Gateway 1000T where c = card, and u = unit.
...		
CLS	MTA	Maintenance allowed Class of Service

Table 51
LD 17: Define Login Types in History File.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	I/O device data
ADAN	NEW CHG OUT HST	Action Device And Number Change the History File
SIZE	(0)-65534	Size of the file
USER	ADM INS USR XADM XINS XUSR	Access levels to be stored in the History File, Administrator, Installer, or User Precede entry with X to remove SBA access level from printing in the History File (see Note)
Note: Only accepted if ADMINSET package is equipped.		

Table 52
LD 17: Increase the Maximum Number of Logins.

Prompt	Response	Description
REQ	CHG	Change
TYPE	PARM	Parameters data
...		
SBA_ADM_INS	0-(1)-2 0-(2)-64	Maximum Administrator and/or Installer logins allowed at one time (see Note) For Small Systems For Large Systems
SBA_USER	0-(10)-20 0-(100)-500	Maximum User logins allowed at one time (see Note) For Small Systems For Large Systems
Note: Only accepted if ADMINSET package is equipped.		

Table 53
LD 17: Increase buffers.

Prompt	Response	Description
REQ	CHG	Change
TYPE	PARM	Parameters data
...		
500B	75	Number of output buffers

Table 54
LD 15: Enable use of Station Control Passwords.

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	FFC	Flexible Feature Code
...		
SCPL	0-8	Set Station Control Password length to a non-zero value (default 0)
...		
SBUP	(YES) NO	(Enable) disable use of Station Control Passwords for Set-Based Administration User level access. Inputting YES means Users on this customer must dial the User FFC followed by the Station Control Password to access User level changes. If the response is NO, users only need to dial the User FFC (see Note 1).
PWD2	xxxx	If a response other than <cr> is entered for SBUP, the PWD2 password must be entered for confirmation (see Note 2).
Note 1: Only prompted if the ADMINSET package is equipped and ACPL is greater than 0. ***Note 2:*** Only prompted if the response to SBUP is not <CR>.		

Table 55
LD 10, LD 11: Assign User Access Allowed Class of Service.

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	xxxx	Type of telephone to be changed.
TN	l s c u c u	Terminal number Format for Large System and CS 1000Esystem, where l = loop, s = shelf, c = card, and u = unit. Format for Small System, Call Server 1000S system, and Media Gateway 1000B, and Media Gateway 1000T where c = card, and u = unit.
...		
SCPW	xxxx	Station Control password for this set
CLS	(ULAD) ULAA	(Deny) Allow User level access to Set-Based Administration.

Table 56
LD 18: Assign User FFC to ABCD Key.

Prompt	Response	Description
REQ	NEW	Add
TYPE	ABCD	abcd key information
TBNO	1	Table number 1
PRED	YES	Data for predial keys
A	USER	Assign User FFC to key A

Single Terminal Access

Single Terminal Access (STA) provides integrated access to Operations, Administration, and Management (OA&M) functions for the systems it monitors. This reduces the number of physical devices needed to administer a system and its subsystems.

The STA application can co-reside with other MSDL applications to ensure flexible use of MSDL port resources. Refer to *Circuit Card: Description and Installation (NN43001-311)* for further information.

Terminology

Single Terminal Access introduces several technical terms. Definitions are provided here for convenience.

Admin Terminal Port

The MSDL port to which the STA Admin Terminal is connected.

STA Admin Terminal

A special-purpose STA terminal configured on port 0 of the STA-equipped MSDL. This is the only terminal that can perform STA port-level configuration and maintenance, although it can also be used as an STA Regular Terminal. Each STA must have one STA Admin Terminal.

STA Monitored System

The system and attached subsystems are connected to the STA-equipped MSDL card under the supervision of the STA Admin Terminal.

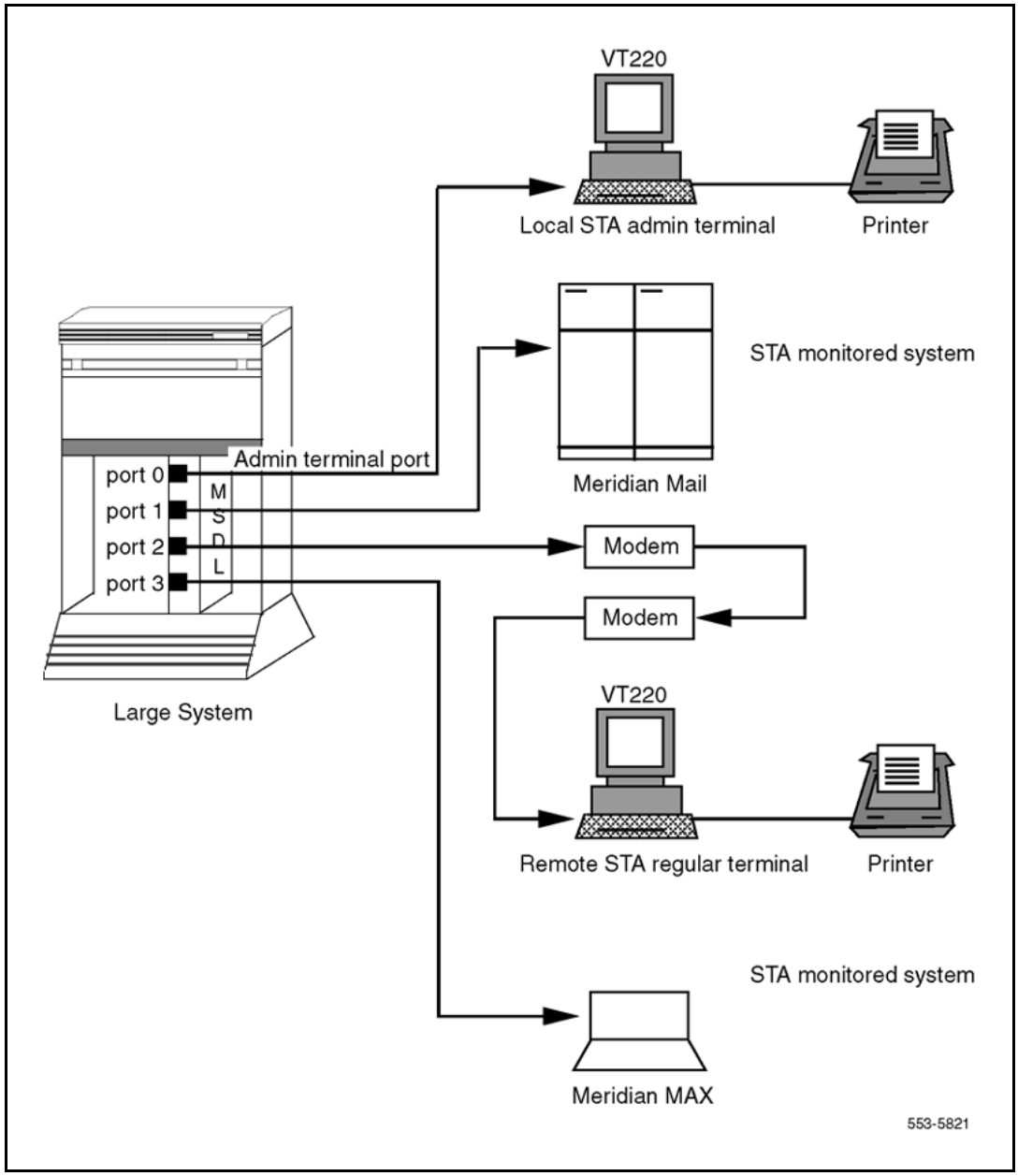
STA Regular Terminal

An STA Terminal, in addition to the STA Admin Terminal, from which a technician can perform integrated system access functions.

STA Terminals

Local or remote VT220s or equivalents that are connected to STA-equipped MSDLs.

Figure 16
An STA-monitored system with STA administration and regular terminals



Functions

STA provides the following major functions:

- Session switching

  STA users can switch between active sessions on multiple connected STA-monitored systems.

- User interface

The menu-driven user interface lets the user monitor and change communication parameters, establish a shadow connection for monitoring an existing connection, manage sessions, and perform maintenance operations from a VT220 terminal.

- Autobauding and data rate adaptation

  STA supports connections between ports with different baud rates. For example, an STA terminal at 9600 baud can connect to Meridian Mail at 2400 baud. STA supports up to 150 buffers of approximately 50 bytes each for data rate adaptation.

  Furthermore, STA is capable of detecting and matching the baud rate of a connected local or remote terminal, on a per port basis. For example, the STA application can receive input at one data rate and output it at another. The mechanism dynamically allocates and releases buffers for temporary storage of these data streams. To prevent data loss through buffer overflow, the mechanism includes XON/XOFF functionality. See “XON/XOFF handling” (page 123).

- MSDL port sharing

  MSDL ports (except for the MSDL SDI) that are not used by STA are available for configuring other MSDL applications.

- Multiple connectivity

  With multiple configured STA terminals, each can establish multiple, simultaneous connections to its monitored systems. For access, STA uses the MSDL SDI interface. Subsystem access does not require system involvement.

- Autorecovery and database protection

  STA includes procedures for autorecovery following fault conditions. Because the STA database resides in a protected data store, recovery does not require reconfiguring the database. Port-level configuration information is uploaded from the STA on the MSDL.

- Printer connection

  The STA (VT220) terminal supports a parallel printer as an option, supporting the Print Screen function within STA, as well as accepting output from the STA-monitored system (such as Meridian Mail). Depending on their needs, STA users can direct data arriving at the VT220 to both the printer and the screen (Auto Print Mode), to just the screen (Normal Mode), or to just the printer (Print Controller Mode).

STA supports two kinds of terminals, administration and regular. The administration terminal is responsible for initialization, configuration, and maintenance of STA ports. The STA regular terminal can perform a subset of the STA administration terminal’s functions, as shown in Table 57 "STA functions by terminal type" (page 154).

Table 57
STA functions by terminal type

Terminal Type	Functions Supported
STA Admin	Add to, change, and view STA port-level configuration Perform STA port-level maintenance View STA port status Establish and discontinue connections
STA Regular	View STA port-level configuration View STA port status Establish and discontinue connections

Operating parameters

Up to two STA terminals (one administration terminal and one regular terminal) are supported per STA application. The STA administration terminal must first be configured as an MSDL SDI terminal on port 0 of the MSDL through LD 17.

To avoid contention, the two terminals cannot be configured with the same priority. By default, the STA administration terminal is assigned the higher priority. Assigning a high priority to the regular terminal prevents the administration terminal from disabling the regular terminal port while in session.

Only one STA application per MSDL is allowed. Up to 16 independent STA applications per system are allowed. Up to three STA subsystem connections are supported; this maximum is restricted by the number of ports supported on a single MSDL card. See Table 58 "Possible port assignments on the STA-equipped MSDL" (page 154) for possible port assignments.

Table 58
Possible port assignments on the STA-equipped MSDL

	Connected Systems or Residing Applications			
MSDL Applications	**Port 0**	**Port 1**	**Port 2**	**Port 3**
STA (1 terminal)	STA Admin	3 STA-monitored systems		

Table 58
Possible port assignments on the STA-equipped MSDL (cont'd.)

	Connected Systems or Residing Applications			
MSDL Applications	**Port 0**	**Port 1**	**Port 2**	**Port 3**
STA (1 terminal) plus other MSDL applications	STA Admin	2 STA-monitored systems + 1 MSDL application or 1 STA-monitored system + 2 MSDL applications		
STA (2 terminals)	STA Admin	2 STA-monitored systems + 1 STA regular terminal		
STA (2 terminals) plus 1 other MSDL application	STA Admin	1 STA-monitored system + 1 STA regular terminal + 1 MSDL application		

Single Terminal Access supports the following as STA-monitored systems:

- Host: The system on which STA is configured; no MSDL port is used (connection is through the backplane)
- Application Modules (AEM) for CCR, Meridian 911, and Meridian Link, each requiring one MSDL port
- Meridian MAX and Meridian Mail, each requiring one MSDL serial port
- Other equipment supporting a VT100 or VT220 terminal interface

All STA terminals, including the STA administration terminal, must be VT220 or equivalent. The STA administration terminal requires support for 8-bit data and Line Mode Editing (LME). STA-monitored systems must support VT100 and higher terminal types. The STA user interface supports emulation modes (EM100 and EM200 with either 7- or 8-bit controls) as part of the port configuration.

The STA administration terminal cannot be any of the following MSDL SDI user types: PMS, APL, HSL, CDR, or PRT.

Information exchanged between systems during a session can be lost if the total buffer area for data rate adaptation (over 5000 bytes) overflows. The XON/XOFF function operates within this buffer limitation.

Because the XON/XOFF function is not supported by all STA-monitored systems, STA users should verify the compatibility of data rates between devices before making connections.

If the system performs a sysload when STA is enabled, the SYSLOAD and INIT messages appear only on the terminal connected to the system.

The STA automatic logout mechanism may not operate for STA-monitored systems, such as Meridian Mail, that do not have logout sequences.

When the printer on the VT220 is operating, users should avoid switching session connections. Any disruption of the normal print job process, which includes an opening command, data stream, and terminating command, may cause printer errors. The loss of a terminating command may have a negative impact on subsequent print jobs.

Feature interactions

System fault management

This procedure sends an alarm message to the STA application when fault conditions occur. STA rings the bell and displays the message to alert the user.

MSDL SDI

STA uses MSDL SDI to handle I/O traffic for system access.

Feature packaging

Single Terminal Access (STA), package 228, requires the following packages:

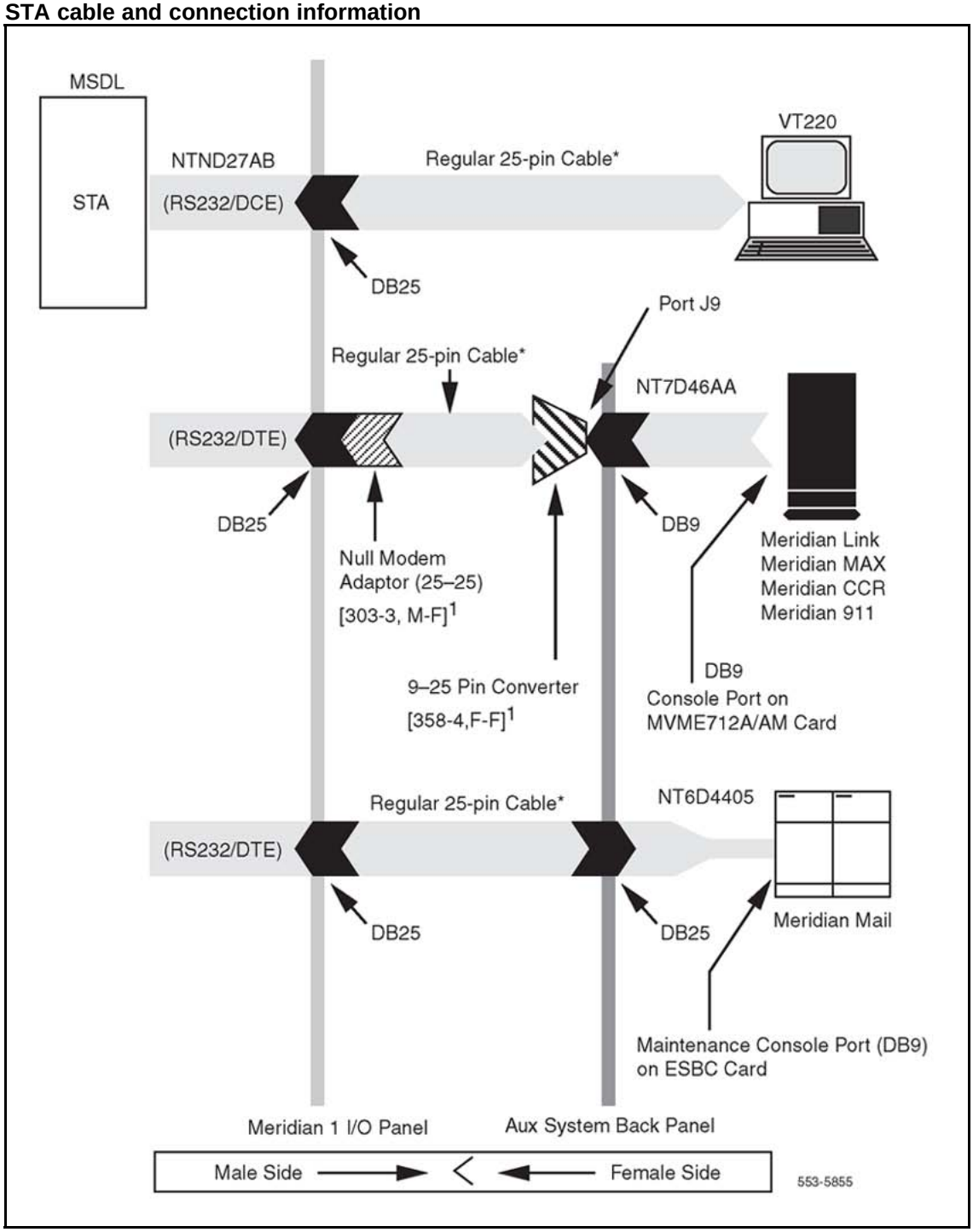
- Multi-purpose Serial Data Link (MSDL) package 222
- MSDL Serial Data Interface (MSDL SDI) package 227

Feature implementation

STA requires specific cabling and connections, as shown in Figure 17 "STA cable and connection information" (page 157). Be sure that MSDL card number (DNUM) switch settings do not conflict with other I/O devices, and that all DIP switches are correctly set.

See Figure 20 "STA planning form" (page 172)for assistance in preparing for an STA implementation.

Figure 17
STA cable and connection information



After completing the planning form, and preparing the MSDL card (DNUM switch settings and DIP switches) and cables, use the following steps to implement STA:

Step	Action
1	Verify that MSDL package 222, MSDL SDI package 227, and STA package 228 software are loaded.
2	Use LD 17 to configure a TTY on the MSDL SDI, making sure the configuration is set for 8-bit operation, and that Line Mode Editing and Autobauding are enabled. See “MSDL Serial Data Interface” (page 121) for assistance.
3	Prepare a VT220 terminal for this port. “Terminal setup for STA” (page 169) shows the setup for a VT420 terminal. Table 59 "Recommended setup for the STA terminal" (page 158) shows the recommended general setup for the STA terminal. Items appearing in bold are of particular importance.

Table 59
Recommended setup for the STA terminal

General Parameters:	
Parameter	**Default STA Terminal Setup**
Terminal Mode	**EM200, 8-bit control**
On-line	Yes
Columns	80
Smooth Scroll	**No**
Cursor Off	No
Inhibit Auto Wrap	Yes
New Line	No
Multi Page	No
Interpret Control	Yes
User Features Lock	No
User Define Key Lock	No
Numeric Mode Keypad	Yes
Normal Mode Cursor Key	Yes
National Character Set	No
Frame Rate	72
Display Off After	15
Terminal ID	**VT220**
Communication Parameters:	
Parameter	**Default STA Terminal Setup**
Transmit Baud	2400–19200

Table 59
Recommended setup for the STA terminal (cont'd.)

General Parameters:	
Parameter	**Default STA Terminal Setup**
Receive Baud	=XMIT
Data Bits	**8**
Parity	No
Check Parity	No
Port Selection	EIA, Data leads only
XON/XOFF	No
Disconnect Delay	2s
Link Stop Bit	1
Local Echo	No
Unlimited Xmit	No
Keyboard Parameters:	
Parameter	**Default STA Terminal Setup**
Keyboard Language	North American
Data Processing Keys	No
Shift Lock	No
Break	Yes
Auto Repeat	No
Answer Back	Blank
Auto Answer Back	No
ESC Key	**Must be configured**

4 Plug the MSDL into the system and connect the terminal cable.

5 Use LD 37 to enable the MSDL and TTY port. Test the port and screen operation. Then disable the port.

6 Use LD 17 to configure the STA application for the TTY and specify additional ports. Use LD 22 to verify the configuration.

Table 60
LD 17: Configure STA application information.

Prompt	**Response**	**Comment**
REQ	CHG	Change
TYPE	ADAN	Action device and number
ADAN	NEW CHG STA 0–15	Assign an ID # to the STA application (up to 16 are allowed)

Table 60
LD 17: Configure STA application information. (cont'd.)

Prompt	Response	Comment
TTY	0–15	The number of the predefined MSDL SDI TTY
CTYP	MSDL	MSDL card type
GRP	0–7	Network group number for Large Systems
DNUM	0–15	Device number for I/O ports
ADMIN_PORT	0	STA admin terminal port # (must be 0)
LANGUAGE	ENGLISH	Supports only ENGLISH
ADDITIONAL_PORT	P1 P2 P3	Additional port number for STA terminal

7 Use LD 48 to enable the STA. Verify STA user interface operation on the terminal. Refer to "Maintenance commands" (page 164) for detailed commands.

8 Use the STA administration terminal to configure allocated STA ports for STA-monitored systems and regular terminals.

9 Configure STA port information:

- Before configuring STA ports, fill out the Figure 20 "STA planning form" (page 172). Also, arrange the port configuration using the information in Table 61 "Recommended port configurations for STA-monitored systems" (page 167).
- Use Change Port Configuration from the **STA Main Menu** to assign a system port for Meridian Mail. For details on STA menu operations, see "User interface" (page 164).
- Connect the right cable between the MSDL port and Meridian Mail.
- Use Port Maintenance from the **STA Main Menu** to enable the port.
- Use Connect to Meridian Mail from the **STA Main Menu** to establish a connection.
- Use <Ctrl-R> to refresh the screen.
- Use <Esc-STA> to return to the **STA Main Menu**.

10 If necessary, use LD 22 to print configuration information.

11 Repeat Step 9 to configure other system ports.

Note: An STA port that is neither a Terminal port nor a System port is marked as allocated but not yet configured.

12 Use Change Port Configuration to configure a second terminal port for a modem-connected terminal. Connect the cable and

enable the port using Port Maintenance. Use a remote VT220 and the modem connection to access the system and Meridian Mail.

13 To change STA application or port allocation, load LD 17 and type CHG STA under the ADAN prompt.

--End--

Application and port configuration download

When STA is enabled from LD 48 or background, the STA application configuration and port-level configuration are downloaded to MSDL.

The SDI/STA loadware is downloaded from disks under the following conditions.

System initialization

After system initialization, the Software Download Application (PSDL) checks enabled MSDL cards to see if their applications have the correct loadware versions. If the software version is incorrect, the SDI/STA application is downloaded to the MSDL in background mode.

STA application enabled

When the STA application is enabled from either LD 48 or background, the SDI/STA loadware is downloaded when either of the following is true: The user can specify the Firmware Download (FDL) option.

- if the MSDL does not have the STA application loaded
- if the STA application on the MSDL is a different version from the one resident on the system disk

Connections

After configuring STA-monitored systems and enabling the associated ports, users on STA terminals can establish one of the following connections with monitored systems.

Active connection

An active session is the normal connection mode, during which the STA application performs these operations:

- Receives data from the source and transmits it to its destination.
- Screens the data to remove incoming characters that the system cannot understand.
- Waits for an escape sequence, and if one is detected, sends a logout sequence to the destination STA-monitored system or presenting users with the STA user interface. After disconnection, any data delivered by

the STA application is discarded. Users can leave an original session in login state by not configuring the logout sequence, although this may result in unauthorized access.

A privacy mode option, with a default of "on," is available to prevent other terminals, regardless of priority, from shadowing the session.

Shadow connection

A shadow connection can be established only on an existing active session; it is disconnected when the active session disconnects. In shadow mode a terminal monitors activities between another terminal and an application but cannot access the application itself.

Modem connection

An STA modem connection requires a terminal port configured with RS-232 (or RS-422) DTE interface type and an attached modem. STA tracks the modem's active signals and uses Carrier Detect (CD) as the indication of a call. Therefore, users should configure their modem so that CD is only on when a call exists.

Note: For Hayes-compatible modems, the following initialization command sets the modem to factory default, with answer on first ring, CD up only when a call is present, echo off, no modem status output, and safe storage when power is down: **at&fs0=1&c1e0q1&w**

Using a modem connection requires that you enter a correct login name and password to proceed to the **STA Main Menu**.

Restart

To configure the STA administration terminal on an enabled and running MSDL SDI TTY, first disable the TTY. The TTY begins acting as an STA administration terminal following application-level configuration in LD 17, STA application (LD 48) implementation, and the download of new parameters onto the MSDL. Instead of enabling the STA application, users can INIT the system to download the parameters and bring up the STA application and administration terminal.

If the STA application is up and running during a restart, the MSDL STA application continues to operate, although only communication from the system to the STA application is supported. In this case, even if you change the STA application-level configuration, it is not downloaded.

If the STA application is up and running, and MSDL base code or the STA application must be downloaded, then STA is temporarily suspended. After an INIT, the STA application is restored.

If the application is not up and running, then a SYSLOAD INIT or manual INIT enables the disabled STA applications and services. After other types of INIT, such as watchdog timeout or response timeout INIT, the STA application remains disabled.

A manual INIT after STA administration terminal parameter changes downloads the modified parameters to the MSDL. STA ports are temporarily disabled for download, then enabled with new parameters. If another TTY is connected separately to the same system, users can download modified parameters by disabling and enabling the STA application.

The STA autorecovery mechanism tries to recover the application after a fault is found and cleared. If the autorecovery process fails three times in a row, the STA application enters system disable state until midnight recovery.

Disabling and removing

The administration terminal can disable a single STA port. LD 48 is required for users who want to disable the STA application. Users can then remove STA-monitored system ports with the administration terminal and use LD 17 to eliminate the STA application.

To disable and remove STA completely:

Step	Action
1	Use LD 48 to disable the STA application.
2	Remove the STA application using LD 17.

--End--

To remove an MSDL port from STA:

Step	Action
1	Use LD 48 to disable the STA application.
2	Use LD 17 to remove the port.

--End--

Feature operation

Maintenance commands

The three classes of maintenance commands for the STA application are MSDL card, STA application, and STA port.

MSDL card commands

Commands in LD 37, LD 42, LD 48, and LD 96 perform the enable, disable, reset, and status reporting operations for maintaining the MSDL card. These commands function identically for STA as for SDI, DCH, and AML.

STA application commands

Commands in LD 48 provide enable, disable, and status reporting operations for the STA application. The commands include the following:

- DIS STA to disable an STA application.
- ENL STA (FDL) to enable an STA application (and force the application to be downloaded). Without the FDL option, the application is downloaded only when needed.
- MAP STA to view information relating to an STA application.
- STAT STA to view the status of an STA application and its ports.

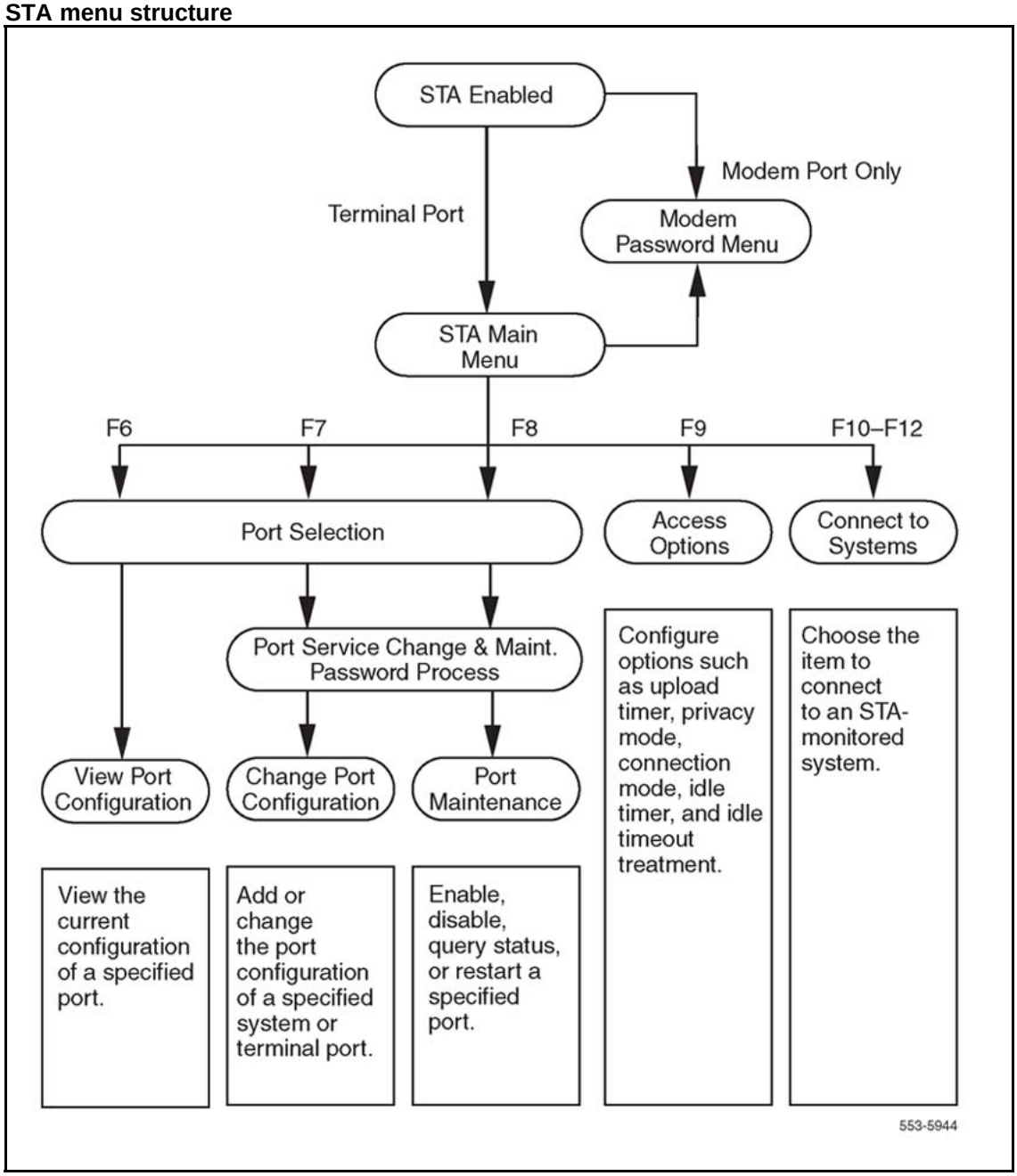
STA port commands

Commands found in the STA user interface provide enable, disable, and status reporting operations on a per port basis, as described in the next section.

User interface

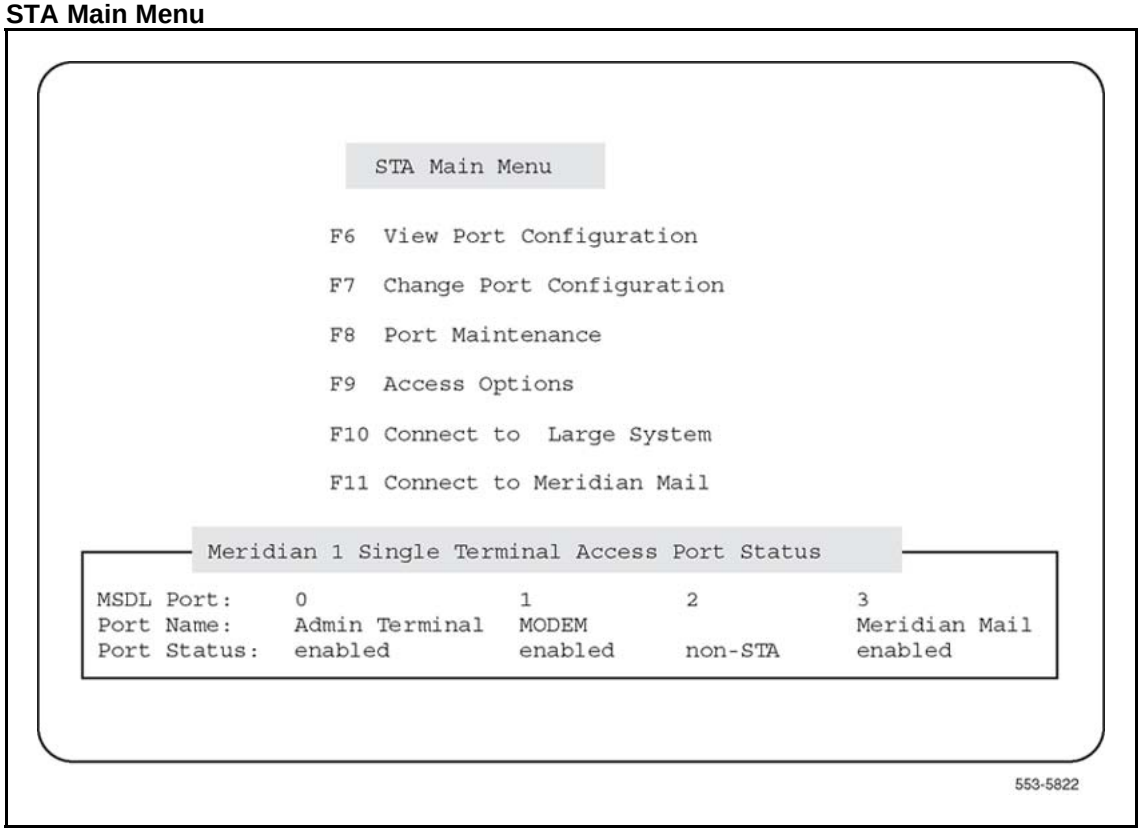
The user interface includes the **STA Main Menu** and several submenus. Figure 18 "STA menu structure" (page 165) shows the structure of the STA menus.

Figure 18
STA menu structure



To select an STA operation from the **STA Main Menu** (see Figure 19 "STA Main Menu" (page 166)), either press the designated function key or move the highlight bar to an operation and press <CR>.

Figure 19
STA Main Menu



F6 View Port Configuration

This operation displays the following configuration information for the selected port: number, type, name, baud rate, data bits, stop bits, and interface. The display for terminal ports includes xon/xoff, autobaud, and priority; for system ports, logout sequence, connect sequence, and emulation.

F7 Change Port Configuration

This operation prompts you to select a port and enter name/password information. The password can be a Level 1, Level 2, or LAPW password, depending on what packages are equipped.

> ***Note:*** If LAPW is equipped, the user name can be up to 11 characters and the password up to 16 characters in length. The password is configured under the NPW1, NPW2, or PW00–99 prompts in LD 17. If the LNAME_OPTION is off, no login name is required.

After validating the user's entries, the operation displays the port information. To change an entry, move the highlight bar to the entry, then use the right and left arrow keys to scroll through acceptable values. The exceptions are name, logout sequence, and connect sequence, all of

which require character input. You can view, but cannot change, the STA administration terminal configuration. It must be changed through LD 17 and downloaded when STA is enabled.

Table 61 "Recommended port configurations for STA-monitored systems" (page 167) lists the recommended port configurations for connecting to STA-monitored systems.

Table 61
Recommended port configurations for STA-monitored systems

	Meridian MAX	Meridian Mail	Meridian Link, Meridian 911, or CCR
Port Type	System	System	System
Baud Rate	9600	2400	9600
Data Bits	8	8	8
Stop Bits	1	1	1
Interface	RS232 DTE	RS232 DTE	RS232 DTE
Connect Sequence	Ctrl-R	Ctrl-R	Ctrl-R
Emulation	EM200 8-bit Ctrl	EM200 7-bit Ctrl	EM100 (see Note)
	Note: EM100 emulation mode is required for a VT220 to operate on a VT100-supported STA-monitored system.		

F8 Port Maintenance

This operation prompts you to select a port and enter the system password (unless you have already done so during Change Port Configuration). After the system validates the entries, a submenu appears with selections to enable the port, disable the port, restart the port, and query the port's pin status. For DTE ports, the query shows the status of the Data Carrier Detected (DCD) and Clear To Send (CTS). For DCE ports, the query shows the status of the Data Terminal Ready (DTR) and Ready To Send (RTS).

F9 Access Options

This operation displays the Optional Operational Setup submenu, from which you can specify miscellaneous terminal timing and management parameters. The default parameter values are predefined for STA administration terminals. The default parameter values for STA regular terminals are inherited from the administration terminal.

The parameters and their acceptable values appear in Table 62 "Access Option parameters and values" (page 168).

Table 62
Access Option parameters and values

Parameter	Value	Description
Configuration Upload Wait Time	(None), 2, 5, 10, 30, Infinite	The value indicates the frequency for uploading new port-level configuration data to the system. None causes immediate upload; Infinite never uploads (used for testing). The only way to abort uploading is to disable the STA application.
Privacy Mode	(Off), On	An active session with privacy mode on cannot be shadowed.
Connection Mode	(Active), Shadow	
Idle Timer	(10), 20, 30, 40, 50, 60	The value indicates how many minutes must elapse before a timeout.
Idle Timeout Treatment	(system), STA Main Menu, Configured STA-Monitored System	The value indicates what the terminal connects to or displays when an idle timeout occurs.

F10 Connect to system
This operation causes the STA terminal to connect to the system.

F11: F13 Connect to Meridian Mail
This operation causes the STA terminal to connect to Meridian Mail.

Port Status Information
The lower portion of each menu displays each port's current state:

- Non-STA: The port is not allocated for STA.
- Disabled: The port is either unconfigured or disabled.
- Enabled: The port is ready for connection.
- In Session: The port is in session with another port.
- Wait Enable: The port is being enabled.
- Wait VT220: The terminal port is waiting for the terminal to respond.
- No Modem Call: The port is enabled but no call has been established.
- DTR Down: For DCE only, the (Data Terminal Ready) DTR pin of the port interface pin is low. The connected device needs to be turned on or the cable connected.

- CTS Down: For DTE only, the Clear to Send (CTS) pin is low. The connected device needs to be turned on or the cable connected.
- Autobauding: The port is using autobaud, autobaud scan, or default baud, or awaiting autobauding.

STA modem connection process

Before a modem connection can be established, users must use the modem connection password menu if they want to enter a name and a required password. A name is required if LAPW is equipped and the login name option is on. The password can be a Level 1 or Level 2 password, or an LAPW password.

If you enter more than ten invalid login name/password combinations, the menu locks and accepts no more input. You must reset the link to resume.

Terminal setup for STA

This section contains a summary of the entries on the VT420 setup screens. In addition, please read the following notes for use with Reflection, Wyse terminals, and PROCOMM PLUS [a] software.

Reflection

Reflection fully supports STA operations in its VT220 emulation mode.

Wyse terminals

In its VT220 emulation mode, a Wyse terminal cannot support Meridian Mail.

PROCOMM PLUS

PROCOMM PLUS enables you to map all keys on an extended keyboard to user-defined control sequences. To ensure proper operation, you must configure any such key sequences for a connection before establishing the connection.

Setup Directory screens

Global	Display	General	Comm	Printer	Keyboard	Tab
Clear Display		Clear Comm		Reset Session	Recall	Save
Set-up=English		Canadian (English) Keyboard				Default
Enable Sessions		Disable Sessions		Screen Align		Exit

Global Setup screens

To Next Set-Up	To Directory	
On Line	S1=Comm1	CRT Saver
Comm1=RS232	70Hz	Printer Shared

Display Setup screens

To Next Set-Up	To Directory	80 Columns	Interpret Controls
No Auto Wrap	Jump Scroll	Dark Screen	
Cursor	Block Style Cursor	No Status Display	
Cursor Steady	3x24 pages	24 Lines/Screen	
Vertical Coupling	Page Coupling	Auto Resize Screen	

General Setup screens

To Next Set-Up	To Directory	VT400 Mode, 8 Bit Controls
User Defined Keys Unlocked	User Features Unlocked	8-bit Characters
Application Keypad	Normal Cursor Keys	No New Line
UPSS DEC Supplemental	VT220 ID	
When Available Update		

Communication Setup screens

To Next Set-Up	To Directory	Transmit=2400-19200	Receive=Transmit
Xoff=64	8 Bits, No Parity	1 Stop Bit	No Local Echo
Data Leads Only	Disconnect, 2s Delay	Limited Transmit	
No Auto Answerback		Answerback=Not Concealed	
Modem High Speed=ignore		Modem Low Speed=ignore	

Printer Setup screens

To Next Screen	To Directory	Speed=9600	Printer to Host
Normal Print Mode	NO XOFF	8 Bits, No Parity	1 Stop Bit
Print Full Page	Print National Only	No Terminator	

Keyboard Setup screens

To Next Set-Up	To Directory	Typewriter Keys	Caps Lock
Auto Repeat	Keyclick High	Margin Bell	Warning Bell High

Character Mode <X] Delete Local Compose Ignore Alt

F1 = Hold F2 = Print F3 = Set-Up F4 = Session F5 = Break

, < and . > Keys < > Key ’ ~ Key = Esc

Tab Setup screens

Leave the defaults unchanged.

Figure 20 "STA planning form" (page 172) illustrates an STA planning form.

Figure 20
STA planning form

Date: _____ Boot Code Version: _____

MSDL Serial No: _____ MSDL Device No: _____

STA Logical No: _____ MSDL SDI Logical No: _____

STA Planning Form

	Port 0	Port 1	Port 2	Port 3
Port Type				
Port Name				
Baud Rate				
Data Bits				
Stop Bits				
Interface				
DIP Switch				
Cable				
Terminal Port Only				
Terminal				
Xon/Xoff				
Autobaud				
Priority				
System Port Only				
Logout Seq				
Connect Seq				
Emulation Mode				

553-5856

System Message Lookup of alarm messages

The System Message Lookup Utility provides the ability to lookup system alarm messages online. The utility accepts system alarm mnemonics and provides a descriptive explanation of the event. It supports Look Up Last Error and Look Up Any System Message. See “Feature operation” (page 173) for information about how to use this utility.

Operating parameters

The help text file contains approximately 10 000 entries and requires approximately 1 MB of memory.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature requires System Message Lookup Utility (SYS_MSG_LKUP) package 245.

Feature implementation

There are no specific implementation procedures for this feature except LD 02 – Printing the Alarm Summary report.

Feature operation

At the > prompt, to activate Look Up Last Error, enter

```
err<cr>
```

The system looks up the last error and displays (prints) the associated help text.

At the > prompt, to activate Look Up Any System Messages, enter

```
err ABCDxxxx<cr>
```

where ABCD is the message mnemonic and xxxx is the message identifier. The system looks up the specific error code and displays (prints) the associated help text. If the system does not find the requested message, it issues the following message:

```
Unable to find help text for error:  ABCDxxxx
```

If the message code entered is invalid (that is, it begins with a number, it has more than four alphabetic characters, or contains special characters), then the system issues the following message:

```
ABCDxxxx is not a valid error code.
```

Appendix Warning

WARNING
Do ***not*** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

This section governs the use of the Red Hat Software and any updates to the Red Hat Software, regardless of the delivery mechanism and is governed by the laws of the state of New York in the U.S.A. The Red Hat Software is a collective work under U.S. Copyright Law. Subject to the following terms, Red Hat, Inc. (“Red Hat”) grants to the user (“Customer”) a license to this collective work pursuant to the GNU General Public License. Red Hat Enterprise Linux (the “Red Hat Software”) is a modular operating system consisting of hundreds of software components. The end user license agreement for each component is located in the component’s source code. With the exception of certain image files identified below, the license terms for the components permit Customer to copy, modify, and redistribute the component, in both source code and binary code forms. This agreement does not limit Customer’s rights under, or grant Customer rights that supersede, the license terms of any particular component.
The Red Hat Software and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to the Red Hat Software and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The “Red Hat” trademark and the “Shadowman” logo are registered trademarks of Red Hat in the U.S. and other countries. This agreement does not permit Customer to distribute the Red Hat Software using Red Hat’s trademarks. If Customer makes a commercial redistribution of the Red Hat Software, unless a separate agreement with Red Hat is executed or other permission granted, then Customer must modify any files identified as “REDHAT-LOGOS” and “anaconda-images” to remove all images containing the “Red Hat” trademark or the “Shadowman” logo. As required by U.S. law, Customer

represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorizations(s) from the U.S. Government; (d) will not use or transfer the Red Hat Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions. Red Hat may distribute third party software programs with the Red Hat Software that are not part of the Red Hat Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at http://www.redhat.com/licenses/. If Customer does not agree to abide by the applicable license terms for such programs, then Customer may not install them. If Customer wishes to install the programs on more than one system or transfer the programs to another party, then Customer must contact the licensor of the programs. If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. Copyright © 2003 Red Hat, Inc. All rights reserved. "Red Hat" and the Red Hat "Shadowman" logo are registered trademarks of Red Hat, Inc. "Linux" is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.

Appendix
Establish a PPP connection

Using a PPP link to the Signaling Server for remote, single point-of-access

PPP over a dialup modem connection to COM1 on the rear of the Signaling Server Leader is the preferred method of remote, single point of access to the system. For example, a PPP link is used for:

- web browser access to Element Manager on the Signaling Server (for example, configuration changes, installation of patches)
- FTP to transfer files to and from the Signaling Server (for example, binary loadware files for Voice Gateway Media Cards)
- Telnet/rlogin sessions to access system elements on the ELAN subnet using the Signaling Server (for example, Call Server, Voice Gateway Media Cards)

Modem and serial COM port configuration for using PPP link to the Signaling Server

For the best performance of the IP-based management clients (such as the Element Manager Web browser, Telnet, rlogin, and FTP) over the PPP link to the Signaling Server, use a V.34bis, V.90, or V.92 modem at both ends of the dialup connection. Ensure that both modems are configured to enable the following:

- hardware flow control

  Note: For hardware flow control, you must use a straight-through (not a null modem) RS232 cable with full RS232 modem control signals, including Clear to Send (CS or CTS) and Request to Send (RS or RTS). The Signaling Server COM1 and COM2 serial ports are equipped with DB-9 male connectors operating as RS232 Data Terminal Equipment (DTE).

- modem error control (ARQ)
- modem data compression

Different operating systems use different names for the serial ports. Table 63 "Serial port name by operating system" (page 178) shows the name of serial ports on the Signaling Server.

Table 63
Serial port name by operating system

Serial Port	Windows	Linux	Solaris	VxWorks
rear	COM1	/dev/ttyS0	/dev/ttya	/tyC0/0
front	COM2	/dev/ttyS1	/dev/ttyb	/tyC0/1

Note: The Microsoft Windows nomenclature is used in this section.

Table 64 "Maximum bidirectional connect speed of modem types" (page 178) shows the maximum bidirectional modem connect speed over a high quality dialup telephone connection for the V.34bis, V.90, and V.92 modems.

Table 64
Maximum bidirectional connect speed of modem types

Modem type	Maximum bidirectional connect speed
V.34bis modem	33.6 kbps
V.90 modem	33.6 kbps
V.92 modem (operating in V.PCM mode)	48.0 kbps

Modem serial port speeds

The serial port speeds for the remote PC and the Signaling Server must be correctly set.

Modem serial port speed for the Signaling Server

The modem must be installed on the Signaling Server's COM1 (rear) serial port. This allows you to observe the startup messages that are displayed when the Signaling Server performs a cold or warm reboot.

The modem serial port speed for the Signaling Server's COM1 port must be configured to exactly 38400 bps (not higher) using the Signaling Server "stty" command from the oam> CLI on Signaling Server COM1 (rear) or COM2 (front).

- Using the stty command from either the COM1 or COM2 serial port changes the speed of both Signaling Server COM ports.
- Using the stty command from a Telnet terminal connected to the Signaling Server does not change the speed of COM1 and COM2.

Procedure 4
Configuring the modem serial port speed for the Signaling Server

Step	Action
1	Log in to the OAM shell.
2	Issue the stty command and configure the serial port speed of COM1 to 38 400 bps. `oam> stty 38400`

--End--

Modem serial port speed for the remote PC

The modem serial port speed for the remote PC running the Dialup Networking client must be configured to 38400 bps or higher. Use the **Dialup Networking Client** to configure the speed. Refer to the **General** tab of the **Dialup Networking Client** properties; see “Modem configuration” (page 38).

Modem Configuration Example: US Robotics Sportster Fax modem 56K

This example refers to US Robotics Product ID 00568603. Read and follow the steps in the technical reference for the modem that you are installing.

The modem must be configured to:

- end Data hardware flow control only
- ignore Request To Send (RTS)

For normal operation of the modem that is connected to COM1 on the Signaling Server, the modem DIP switch settings are ALL UP (OFF) except for DIP switch 1 and 4 DOWN (ON). See Table 65 "DIP switch settings" (page 179).

Table 65
DIP switch settings

DIP Switch	Position	Description
DIP Switch 1	Down (ON)	Modem ignores Data Terminal Ready
DIP Switch 2	Up (OFF)	Modem displays verbal result codes
DIP Switch 3	Up (OFF)	Modem suppresses display of result codes
DIP Switch 4	Down (ON)	Modem suppresses display of result codes
DIP Switch 5	Up (OFF)	Modem answers if S0=1 or greater

Table 65
DIP switch settings (cont'd.)

DIP Switch	Position	Description
DIP Switch 6	Up (OFF)	Modem sends Carrier Detect signal on serial port when carrier is present
DIP Switch 7	Up (OFF)	Modem loads the previously modified and stored NVRAM configuration profile (Y0 or Y1), or the read-only factory configuration profile (Y2, Y3, or Y4) selected by the Y parameter. You must use the modem AT command AT Y0 to select NVRAM stored configuration profile 0 which has been configured to enable Send Data hardware flow control only.
DIP Switch 8	Up (OFF)	Modem ignores AT commands (Dumb Mode)

DIP switch settings are read and applied when:

- The modem is powered on.
- The modem is reset by using the ATZn command.

AT Command Set

To temporarily use the AT command set on the modem that connects to Signaling Server's COM1 port, you must:

Step	Action
1	Connect a terminal directly to the modem.
2	Set DIP switch 8 DOWN (ON).
3	Power the modem OFF/ON.

--End--

The modem then responds to the AT command set; however, type carefully because the modem still suppresses local echo of AT commands entered from the terminal and also suppresses display of result code **OK**. DIP switches 3 and 4 can be adjusted, but typing carefully will work.

Procedure 5
Using the AT command set

Step	Action
1	Type **`AT Z4`** and press **Enter** to reset default S registers and load factory configuration profile 1 which is the hardware flow control template.

Factory profile 1 enables hardware flow control for both Send Data and Receive Data.

Note: You must disable Receive Data hardware flow control to operate the modem on the Signaling Server COM port.

2 Type **AT &R1** and press Enter to configure the modem to ignore Request To Send (RTS).

This disables Receive Data hardware flow control and allows you to log into the Signaling Server COM port.

3 Type **AT &W0** and press Enter to store the modified hardware flow control configuration in NVRAM stored profile 0.

4 Type **AT Y0** and press Enter to set Y0.

If DIP switch 7 is UP (OFF) upon resetting, the modem loads NVRAM stored configuration profile 0 which enables Send Data hardware flow control only.

5 Type **ATZ** and press Enter to reset the modem and load the Y0 Send Data hardware flow control configuration according to DIP switch 7 UP (OFF).

6 Type **AT I4** and press Enter to display the current modem configuration and verify the settings Y0, H1, and R1.

If the settings are not correct, repeat step 1 through step 6. Read and follow the technical reference for the modem you are installing to configure it for Send Data hardware flow control only.

--End--

Configuring a Dial-up Networking PPP Client for remote access to the Signaling Server

Use Procedure 6 “Configuring a Dial-up Networking PPP client for remote access to the Signaling Server” (page 181) to configure a Dialup Networking PPP Client on the remote PC running MS Windows 2000 or other MS Windows operating system with MS Internet Explorer version 5.5 or later.

Note: Enable or disable properties as recommended in; leave other properties with the default settings (that is, do not change them).

Procedure 6
Configuring a Dial-up Networking PPP client for remote access to the Signaling Server

Step	Action
1	Select **Start > Settings > Control Panel**.

2 Double-click **Network and Dial-up Connections**.

3 Double-click **Make New Connection**.

The **Network Connection Wizard** window opens. Click **Next**.

4 Select the **Network Connection Type**. Click **Next**.

5 Select dial-up modem connection. Click **Next**.

6 Right-click the connection and select **Properties**.

The **Properties** window for the newly created dial-up connection appears. The **Properties** window has five tabs. Configure the properties as outlined in the following steps.

7 On the **General** tab, click the Configure **button**.

The **Modem Configuration** window opens

8 Configure the following:

a Set **Maximum speed (bps)** to 38400, 57600, or 115200.

b Select **Enable hardware flow control**.

c Select **Enable modem error control**.

d Select **Enable modem data compression**.

e Do not select **Show terminal window**.

f Do not select **Run script**

g Select **Enable modem speaker**.

h Click **OK**. The Dial-up Connection window reappears.

9 Select the **Options** tab.

a Enable **Display progress while connecting**.

b Disable **Prompt for name and password**.

c Disable **Include Windows logon domain**.

d Enable **Prompt for phone number**

e Leave all the other properties with the default settings.

10 Select the **Security** tab.

a Under **Security options**, select **Typical (recommended settings)** radio button.

b Under **Interactive logon and scripting**:

1. Enable **Show terminal window**.
2. Ensure that Run script is not checked.

11 Select the **Networking** tab.

a Under **Type of dialup server I am calling**:, select PPP, Windows 95/98/NT4/2000, Internet.

b Click the **Settings** button. The PPP Setting window opens.

1. Uncheck the **Enable software compression** checkbox.
2. Click **OK** to close the PPP Settings window.

c Under **Components used by this connection**:

1. Enable **Internet Protocol (TCP/IP)**.
2. Disable **File and Printer Sharing for Microsoft Networks**.
3. Disable **Client for Microsoft Networks**.
4. Disable any other components.

d Highlight Internet Protocol (TCP/IP) and click the **Properties** button.

The **Internet Protocol (TCP/IP) Properties** window opens.

1. Select the **Obtain IP address automatically** radio button.
2. Select the **Obtain DNS server address automatically** radio button.

e Click the **Advanced** button.

The **Advanced TCP/IP Properties** window opens.

f On the **General** tab:

1. Disable **Use default gateway on remote network**.
2. Enable **Use IP header compression**.

g Select the **Options** tab.:

1. Click the **Properties** button. The **IP Security** window opens.

h Check the **Do not use IPSEC** radio button.

i Click **OK** to save the settings and close the IP Security window.

j Click **OK** to save the settings and close the Advanced TC/IP Settings window.

k Click **OK** to save the settings and close the Internet Protocol TCP/IP Properties window.

l Click **OK** to save the settings and close your dial-up connection window.

--End--

Configure the Call Server route

Use "Configure the Call Server route" (page 184) to configure the Call Server route for remote single point of access using the Signaling Server PPP link.

Procedure 7
Configure the Call Server route

Step	Action
1	Log in to LD 117.
2	Issue the following command: `NEW ROUTE <Signaling Server ELAN network interface IP Address>`
3	Issue the following command: `PRT ROUTE`
4	Issue the following command: `ENL ROUTE n`
5	Issue the following command: `STAT ROUTE`
6	Verify presence of route to destination xxx.xxx.xxx.xxx by Gateway <Signaling Server's ELAN network interface IP Address>.

--End--

Configure Voice Gateway Media Card ELAN subnet route

Use Procedure 8 "Configure the Voice Gateway Media Card ELAN subnet route" (page 184) to configure the Voice Gateway Media Card ELAN subnet route for remote single point of access using the Signaling Server PPP link.

Procedure 8
Configure the Voice Gateway Media Card ELAN subnet route

Step	Action
1	Connect to each Voice Gateway Media Card and log in to the VxWorks shell.
2	Issue the following command to go to the root directory: `cd "/C:"`
3	Create a new directory called etc by issuing the following command:

```
mkdir "etc"
```

4 Use the change directory command to go to the etc directory.

```
cd "etc"
```

5 Issue the following command:

```
copy 0,"startup"
```

6 Issue the following command:

```
routeAdd "137.135.3.2","<Signaling Server ELAN network interface IP Address>"
```

7 Press Ctrl-D.

8 Issue the following command:

```
copy "startup"
```

9 Verify correct contents of /C:/etc/startup script file.

10 Issue the **cardReset** command.

11 Verify the successful execution of startup script (immediately following the VxWorks startup banner.)

12 Login to IPL> shell and enter the **routeShow** command. Verify presence of HOST ROUTE to Destination 137.135.3.2 by Gateway <Signaling Server ELAN network interface IP Address>.

--End--

Use remote single point of access

Use Procedure 8 for remote single point of access using the Signaling Server PPP link.

Procedure 9
Using Remote Single Point of Access

Step	Action
1	Once the Dialup Networking Client connects to the modem on the Signaling Server:
	a Use the interactive login terminal window to log in to oam> shell
	b Enter the **ppp** command without parameters.
	`oam> ppp`
	Table 66 "Result of entering ppp command without parameters" (page 186) shows the result of entering the ppp command.

Table 66
Result of entering ppp command without parameters

If you are connected to the:	Entering ppp without parameter gets:
rear COM port (/tyCo/0) on the Signaling Server	• the default Local IP address 137.135.3.1 for the Signaling Server ppp3 interface • the default Remote IP address 137.135.3.2 for your remote PC PPP interface
front COM port (/tyCo/1) on the Signaling Server	• the default Local IP address 137.135.5.1 for the Signaling Server ppp5 interface • the default Remote IP address 137.135.5.2 for your remote PC PPP interface

c Click the **Done** or **Continue** button in **PPP Client Interactive Login Terminal** window.

WARNING
After entering the ppp command you will see the ASCII display of the binary PPP protocol.

Once you have entered the ppp command, there is a window of *approximately 50 seconds* for you to click the Done or Continue button, and for the PPP service on the Signaling Server and the PPP dialup client on the remote PC to establish the PPP link.

If you allow the window to time out, you must cancel and try again.

2 From the remote PC, start a primary Telnet connection to IP address 137.135.3.1 on the Signaling Server.

From within a primary Telnet session on the Signaling Server you can establish:

- a secondary nested rlogin session to the Call Server, or
- a secondary nested Telnet or rlogin session to another Signaling Server or to any Voice Gateway Media Card using the ELAN network interface.

When you exit the secondary rlogin or Telnet session, you are still logged in to the primary Telnet session on the Signaling Server.

Note: You can have multiple logins to the oam> and PDT> shells on a single Signaling Server, but only one login at a time to the VxWorks shell on the Signaling Server.

3 Log in to the oam> shell of the Signaling Server using Telnet to connect the Signaling Server ppp3 local IP address.

4 Use the **IPInfoShow** command to get the ELAN subnet network ID and ELAN network interface subnet mask of the Signaling Server:

```
oam> IPInfoShow
```

The ELAN subnet network ID is the Destination of the NET ROUTE entry that shows the Signaling Server ELAN network interface IP address as the Gateway.

5 Write down the Signaling Server ELAN subnet network ID and ELAN network interface subnet mask.

6 Open a command window on the remote PC.

7 Enter the following command to add an IP route to the ELAN subnet network ID by the Gateway of the PPP network interface IP address of the remote PC (that is, the Signaling Server ppp3 Remote IP address).

```
oam> route add <Signaling Server ELAN subnet network ID>
mask
<Signaling Server ELAN network interface subnet mask>
137.135.3.2
```

Note: This IP route must be added on the remote PC every time a new dialup PPP connection to the Signaling Server is established. The route to the Signaling Server ELAN subnet by the PPP interface is automatically removed from the remote PC IP route table whenever the PPP link is disconnected.

8 Open a web browser on the remote PC and enter the URL of the Element Manager web server on the Signaling Server on the PPP IP address 137.135.3.1/.

9 If there is a Primary or Alternate NRS on the same Signaling Server, you can point the web browser to the NRS on the PPP IP address 137.135.3.1/nrs.

10 Verify that you have:

- created HOST ROUTE entries to Destination 137.135.3.2 by the Signaling Server ELAN network interface IP address Gateway on each of the system elements, and
- added the destination route to the Signaling Server ELAN subnet by the Gateway of the PPP interface IP address 137.135.3.2 on the remote PC

Use Element Manager to establish a direct Telnet session from the remote PC to the Voice Gateway Media Card or other Signaling Servers on the Signaling Server ELAN network interface.

To do this, select **> IP Telephony > Nodes, Servers, Media Cards > Node Maintenance and Reports** and then click the **Virtual Terminal** button.

11 Establish a direct rlogin connection from the remote PC to the Call Server using the Signaling Server ELAN network interface.

If you use an rlogin client such as VanDyke Software CRT 4.0 on the remote PC, you can configure the rlogin connection with the Username: CPSID. This rlogin username, CPSID, bypasses the PDT login on the Call Server and goes straight to the SL1 Overlay login.

12 Once logged in to Call Server SL1 Overlay command line, use the:

- **LON** command to turn on Line Editing mode
- **LOF** command to turn off Line Editing mode

Note: The Call Server CLI becomes easier to use when SL1 Overlay Line Editing mode is turned on. In Line Edit mode, you can use the Delete key or Ctrl-Backspace keys on the keyboard to correct typing errors on the Call Server Overlay CLI (before pressing <Enter>).

13 You can also establish direct FTP connections from the remote PC to the system elements using the Signaling Server ELAN network interface.

--End--

Nortel Communication Server 1000

System Management Reference

Release: 7.0
Publication: NN43001-600
Document revision: 04.02
Document release date: 15 June 2010

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

www.nortel.com