Meridian 1
Succession 1000
Succession 1000M
Succession 3.0 Software

System Management

Document Number: 553-3001-300
Document Release: Standard 1.00
Date: October 2003

Revision history

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)

Contents

System management applications   127

About this document

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

Subject

This document provides a description of the overall management solution for
Succession 1000M, Succession 1000, and Meridian 1 systems.

Note on legacy products and releases

This NTP contains information about systems, components, and features that
are compatible with Succession 3.0 Software. For more information on
legacy products and releases, click the **Technical Documentation** link under
Support on the Nortel Networks home page:

http://www.nortelnetworks.com/

Applicable systems

This document applies to the following systems:

- Meridian 1 Option 11C Chassis

- Meridian 1 Option 11C Cabinet

- Meridian 1 Option 51C

- Meridian 1 Option 61

- Meridian 1 Option 61C

- Meridian 1 Option 61C CP PII

- Meridian 1 Option 81

- Meridian 1 Option 81C

- Meridian 1 Option 81C CP PII

- Succession 1000

- Succession 1000M Chassis

- Succession 1000M Cabinet

- Succession 1000M Half Group

- Succession 1000M Single Group

- Succession 1000M Multi Group

Note that memory upgrades may be required to run Succession 3.0 Software on CP3 or CP4 systems (Options 51C, 61, 61C, 81, 81C).

System migration

When particular Meridian 1 systems are upgraded to run Succession 3.0 Software and configured to include a Succession Signaling Server, they become Succession 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a Succession 1000M system.

Table 1
Meridian 1 systems to Succession 1000M systems (Part 1 of 2)

This Meridian 1 system...	Maps to this Succession 1000M system
Meridian 1 Option 11C Chassis	Succession 1000M Chassis
Meridian 1 Option 11C Cabinet	Succession 1000M Cabinet
Meridian 1 Option 51C	Succession 1000M Half Group
Meridian 1 Option 61	Succession 1000M Single Group
Meridian 1 Option 61C	Succession 1000M Single Group
Meridian 1 Option 61C CP PII	Succession 1000M Single Group
Meridian 1 Option 81	Succession 1000M Multi Group

Table 1
Meridian 1 systems to Succession 1000M systems (Part 2 of 2)

This Meridian 1 system...	Maps to this Succession 1000M system
Meridian 1 Option 81C	Succession 1000M Multi Group
Meridian 1 Option 81C CP PII	Succession 1000M Multi Group

Note the following:

- When an Option 11C Mini system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Chassis.

- When an Option 11C system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Cabinet.

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

- *Small System: Upgrade Procedures* (553-3011-258)

- *Large System: Upgrade Procedures* (553-3021-258)

- *Succession 1000 System: Upgrade Procedures* (553-3031-258)

Intended audience

This document is intended for individuals responsible for managing Succession 1000M, Succession 1000, and Meridian 1 systems.

Conventions

Terminology

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

- Meridian 1

- Succession 1000

- Succession 1000M

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

- Succession 1000M Chassis
- Succession 1000M Cabinet
- Meridian 1 Option 11C Chassis
- Meridian 1 Option 11C Cabinet

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

- Meridian 1 Option 51C
- Meridian 1 Option 61
- Meridian 1 Option 61C
- Meridian 1 Option 61C CP PII
- Meridian 1 Option 81
- Meridian 1 Option 81C
- Meridian 1 Option 81C CP PII
- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group

The call processor in Succession 1000 and Succession 1000M systems is referred to as the "Succession Call Server".

Conventions used in this document

1   <Pointed brackets> indicate keyboard keys to use. For example, in the following, type "LD 17" and then press the Return key:

LD 17 <cr>

2   UPPER CASE indicates output from the Meridian 1 as well as input entered by the user. For example, in the following, the system prompts for a type, and the user responds with the mnemonic for configuration:

TYPE   CFN

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Meridian 1 Integrated Telephony Gateway Trunk 1.0/Basic Per-Trunk Signaling: Description, Installation, and Operation* (553-3001-116)

- *Meridian 1 Integrated Telephony Gateway Line Card 1.0/IP Telecommuter: Description, Installation, and Operation* (553-3001-119)

- *Circuit Card: Description and Installation* (553-3001-211)

- *IP Peer Networking* (553-3001-213)

- *Branch Office* (553-3001-214)

- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230)

- *System Security Management* (553-3001-302)

- *Set-Based Administration* (553-3001-303)

- *Features and Services* (553-3001-306)

- *Software Input/Output: Administration* (553-3001-311)

- *Optivity Telephony Manager: System Administration* (553-3001-330)

- *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331)

- *Succession 1000 Element Manager: System Administration* (553-3001-332)

- *IP Trunk: Description, Installation, and Operation* (553-3001-363)

- *IP Line: Description, Installation, and Operation* (553-3001-365)

- *Software Input/Output: System Messages* (553-3001-411)

- *Software Input/Output: Maintenance* (553-3001-511)

- *Large System: Overview* (553-3021-010)

- *Large System: Installation and Configuration* (553-3021-210)

- *Large System: Maintenance* (553-3021-500)

- *Succession 1000 System: Installation and Configuration* (553-3031-210)

- *Succession 1000 System: Upgrade Procedures* (553-3031-258)

- *Succession 1000 System: Maintenance* (553-3031-500)

Online

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

http://www.nortelnetworks.com/

CD-ROM

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

Description

Contents

This section contains information on the following topics:

Introduction

As telecommunications systems expand to accommodate more users, the system administrator's role must expand to support new hardware and software options. To make appropriate installation decisions and complete Operations, Administration, and Maintenance (OA&M) tasks efficiently, the administrator must acquire a system-wide perspective of the system and its components. The following is intended to help system administrators and technicians gain that perspective.

I/O architecture

Figure 1 on identifies major elements in the system I/O architecture.

Figure 1
I/O architecture
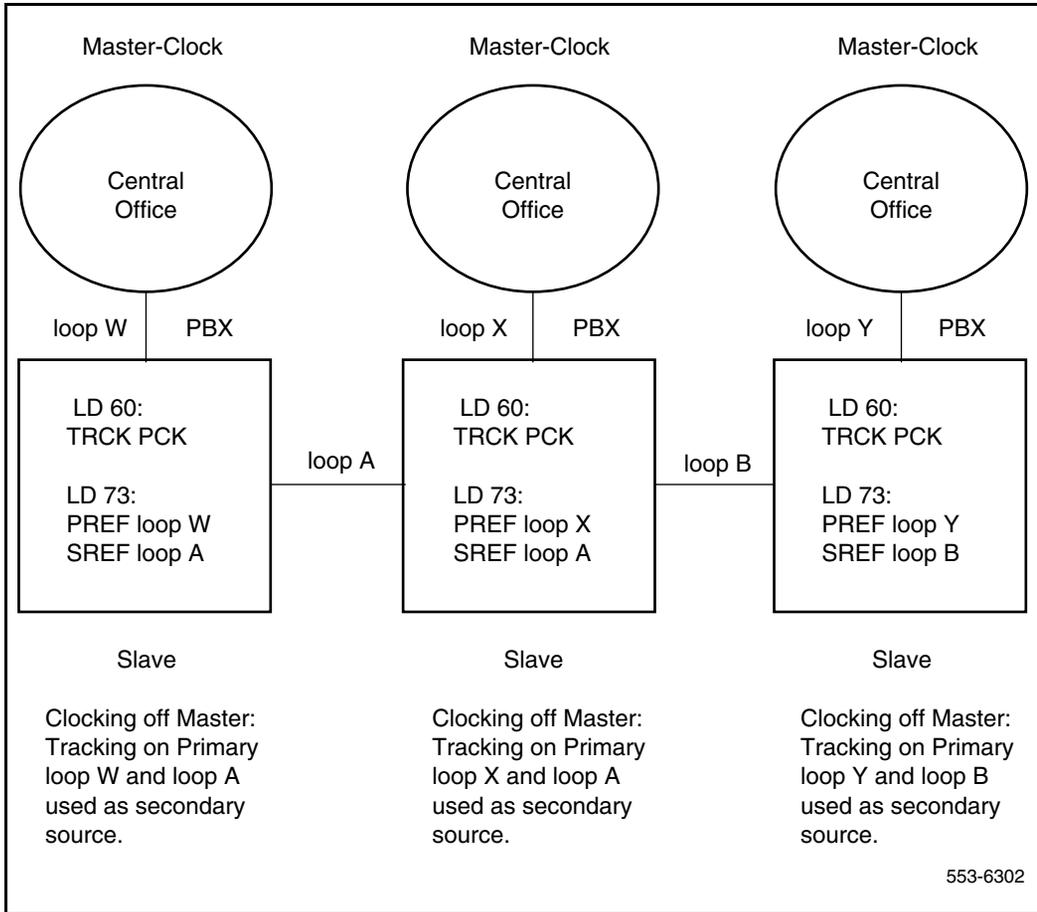
System architecture

The system software provides call processing and feature operation, administration and system management programs, and maintenance and diagnostic programs.

The system architecture consists of the following elements:

- software programs

- firmware programs

- physical (hardware) components

- system configuration data

- system memory and storage

The Central Processing Unit (CPU) loads the basic system software and system configuration data from disk and stores them in Random Access Memory (RAM). Specific programs run as needed to perform various CPU tasks, including administration and maintenance. See Figure 2 on .

Figure 2
System Management Architecture
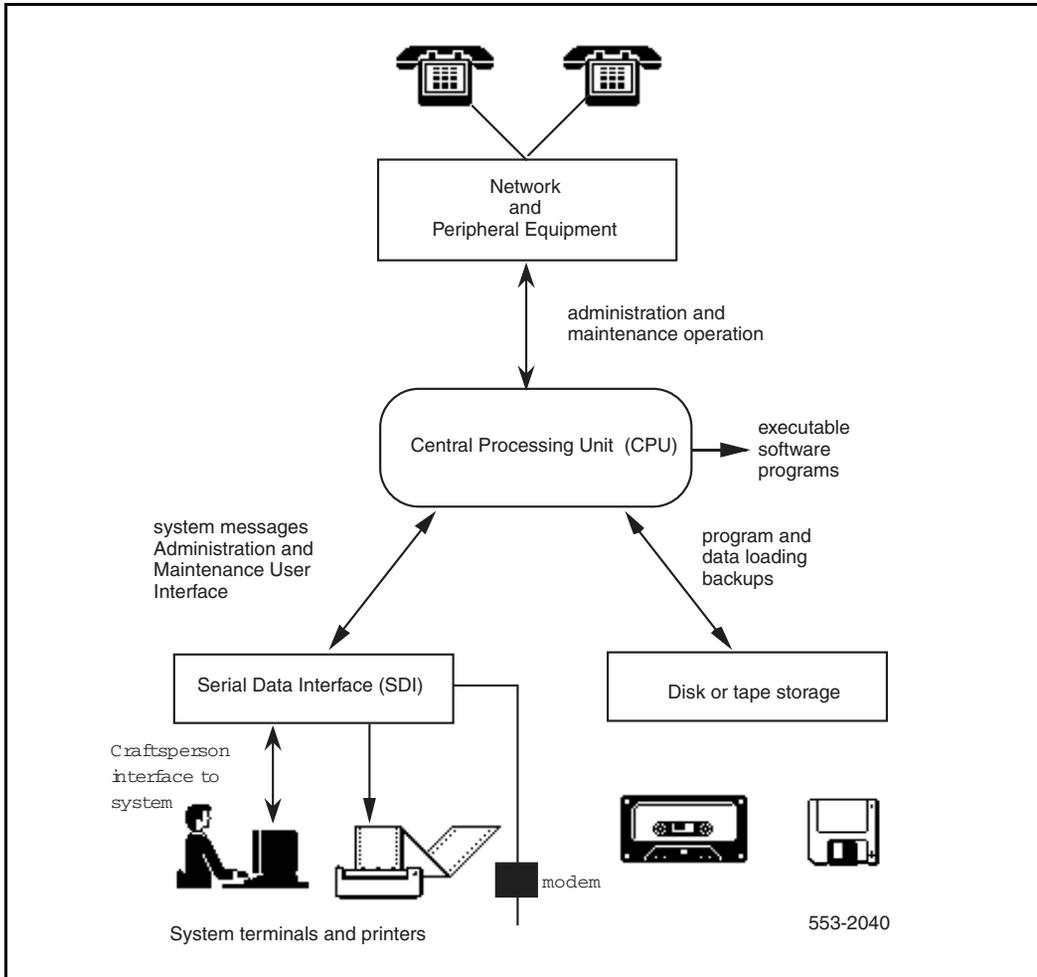
System memory and storage

There are three types of system memory and storage:

• Random Access Memory (RAM)

• Read Only Memory (ROM)

• Auxiliary storage

Random Access Memory

Random Access Memory (RAM) is volatile memory that resides on memory circuit cards associated with each CPU. It stores programs and data for CPU access and system operation. RAM memory is divided into four areas:

• **Program Store** – contains software instructions for call processing and feature operation as well as system management tasks.

• **Protected Data Store** (P-Data) – contains system configuration information, including:

— hardware configuration

— equipped features

Data administered by the technician through system administration programs resides in Protected Data Store. Protected Data Store can be backed up or "datadumped" onto auxiliary storage. Protected data is not affected by system initialization.

• **Unprotected Data** (U-Data) – contains transient call processing data, including:

— call registers maintaining the status of all calls

— TTY login status

— traffic statistics

— idle/busy and key/lamp status of all telephone sets

Unprotected data cannot be saved to auxiliary storage and is refreshed upon system initialization. Preceding each administrative task sequence, the system notifies the user of available P-Data and U-Data.

• **Overlay areas** – contain administration or maintenance programs that are loaded manually by the administrator or automatically by the CPU.

If Overlay Cache Memory is implemented and the system receives a request to load a program, the system checks cache memory for the requested program. If it is in cache memory, its data portion is rapidly copied to the overlay area. A requested program that is not in cache memory is loaded from the disk into the normal overlay area and simultaneously stored into a cache memory buffer, if one is available. If one is not available, the newly requested program overwrites another in the cache memory.

Read Only Memory

Read Only Memory (ROM) is non-volatile memory and resides on a field-replaceable board on the CPU. It includes various system control programs. Software releases and system types require different ROM.

Auxiliary storage

Auxiliary storage provides permanent storage for operating programs and system data. If there is a power loss or a severe system failure resulting in a sysload, the programs and data are reloaded into RAM. Administration and maintenance programs also reside on auxiliary storage and are loaded into RAM as needed.

Auxiliary storage can reside on a floppy disk/CD or hard disk.

Administration changes to protected data must be saved on auxiliary storage using the Data Dump Program (LD 43).

Disk repartitioning

The /p partition on the hard disk is 60 Mbytes. All the program files installed are stored in the new /p partition. All the files currently in the old /p partition, including database files and report files sorted in the /u partition, are not affected. This change occurs during Software Installation, Software Upgrade, and SYNC.

If the installation program detects that the size of the /p partition is smaller than the required size, it automatically repartitions the hard disk. The following messages display after the Installation Tool opening banner is printed on the screen:

```
A software upgrade has been detected.
The /p will be created or repartitioned. The customer
database
will NOT be erased.
>/Repartition of /p in progress.
>Creating block device /p (120000 sectors)
>Initializing device /p
>Hard disk repartition completed

The hard disk on <side #> has been repartitioned!
Now, you may continue with your installation.
```

A new entry, <c>, has been added to the existing Tools Menu to display information about the hard disk and the size of each partition.

This information can also be obtained from "pdt" during normal system operation, with the "scsiDiskStat <cmdu#>" command.

```
This is the Tools Menu for Install. You can select the
tool that is
appropriate. Please select one of the options below.
Please enter:
<CR>-><a> - To set the system date and time.
<b> - To partition the hard disk.
<c> - To display the partition size of the hard disk.
<d> - To go back to the Main Menu.
Enter Choice>
```

If the need to repartition a disk is detected when the SYNC command is invoked from LD 137, the hard disk will be repartitioned in the same way as at the start of Software Installation. The following messages will be displayed:

```
>SYNC
>The standby CMDU does not have the required /p
partition.
The hard disk on <side #> will be repartitioned before
sync'ing.
The hard disk on <side #> has been repartitioned!
```

The IDC command in LD 137 will display the disk drive size in megabytes in addition to the Card ID.

```
>IDC
CMDU0 NT6D64AAXXXX 03 001C SZ:124
```

If a repartitioned CMDU command is used on a system that is running older software, it functions normally. Since the original /p partition is untouched by disk repartitioning, backwards compatibility is maintained.

User interfaces

Contents

This section contains information on the following topics:

Introduction

There are several processors that comprise the system, all being managed by some or all of the following User Interfaces:

- Command Line Interface

- Element Manager

- Optivity Telephony Management

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 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" on

After loading, the administration programs use a step-by-step prompt and response format. The program issues a prompt for input; the system administrator enters the appropriate response through the keyboard, followed by the Return key. The Return key (represented in procedures as <cr>) signals the end of each response. Table 2 shows an example of how to use an administration program.

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 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.
- 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* (553-3001-411).

The *Software Input/Output: Administration* (553-3001-311), *Software Input/ Output: System Messages* (553-3001-411), and *Software Input/Output: Maintenance* (553-3001-511) contain all the prompts and responses, commands and system messages for the Succession 1000M, Succession 1000, and Meridian 1 systems. *What's New for Succession Communication Server for Enterprise 1000* (553-3023-015) contains all the latest prompts and responses, commands and system messages that have been added for Succession 3.0.

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

Element Manager

Each Signaling Server enables access to the system configuration through a web user interface. Element Manager is accessed directly using a web browser or by using the OTM 2.1 navigator which includes integrated links to each Element Manager server in a given network.

Element Manager increases the efficiency of management tasks by organizing parameters in logical groups, where single web pages provide access to information traditionally spread across multiple overlays. Element Manager helps reduce configuration errors by providing a full text description of the parameters (as well as the abbreviations), and simplified choices for selecting parameter values (pre-selected default values, drop-down lists, and indication of range values).

To use Element Manager, direct the web browser to the web server on the Leader Signaling Server. The Element Manager login screen appears. The **/ gk** URL extension of Element Manager, **http://SignalingServerIP/gk/**, provides direct web-page access to Gatekeeper-specific parameters.

The following management tasks are performed using Element Manager:

- **System Status**: Offers the capability to obtain information on the Call Server software version, ISM parameters and packages list. Helps the user to perform maintenance actions on Call Server components (D-channel, MSDL, TMDI, Digital Trunk, Clock Controller, Network and Peripheral, Zone diagnostics, Trunk diagnostic and report log) and IP telephony (Syslog, Report log, OM reports, Telnet, General commands, Status, and Signaling Server report log)

- **Configuration**: Configuration of customer data, trunks and routes (traditionally done using LDs 14, 15 and 16), D-channel and Common Equipment data (LD 17), digital trunk interface (LD 73), Flexible Code Restriction and Incoming Digit conversion (LD 49), zone configuration (LD 117) and IP telephony (IP Line 3.1, Signaling Server).

- **Network Numbering Plan**: Configuration of all ESN data blocks *(LD 86, 87, 90)* for the Call Server as well as the configuration of the Gatekeeper.

- **Software upgrades**: For IP telephony, the capability to view software and firmware versions on components, upload software or firmware to a directory on the Signaling Server, and download new versions to components.

- **Patching**: Offers the capability to download, activate, and deactivate patches for the Call Server, Media Gateway, and IP telephony components.

- **System Utilities**: Includes backup and restore of databases and time and date set.

    Note: Telnet sessions to various IP telephony components (Voice Gateway Media Cards, Signaling Servers) can be established from the Element Management interface.

Optivity Telephony Manager

Optivity Telephony Management (OTM) provides an integrated suite of management tools for configuration, control and analysis of Succession 1000M, Succession 1000, and Meridian 1 networks. OTM is a single-workstation management platform that can scale into a client/server

architecture. It offers both a Windows and web navigator view of the network. It includes several applications such as:

- Station Administration

- Alarms Management

- Call Tracking

- Call Accounting and Billing

- ESN Configuration

- Maintenance

- MDECT

- Traffic Analysis

- List Management

- ITG configuration management

OTM supports a number of utility applications, which are described in "Utilities" on , including the following:

- LDAP

- Corporate Directory

- Inventory management

- Terminal emulation to various components

- Database backup and restore

- Security management

- Data buffering

- Server access

- Overlay pass-through

- Online help

Communicating with the system

Contents

This section contains information on the following topics:

Introduction

System administrators 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, see "Maintenance Telephone" in the *Large System: Maintenance* (553-3021-500) guide.

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

Data communication technologies

The basic interface to a component is the RS-232 maintenance port. Locally, you can connect a maintenance workstation to the RS-232 port, possibly requiring a null modem adapter.

Dial-up modems are used on ports that can establish a Point-to-Point Protocol (PPP) link. A single device connection is robust and simple, but a central connection point promotes ease of use. The following methods promote centralized 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). This enables access to the ELAN.

- Modem router on the ELAN

- Terminal server

- Secure dial-up Remote Access Server (RAS)

- 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 Telnet through a terminal server to individual components on the ELAN, and therefore obtain maintenance access on each device. Figure 3 on illustrates direct modem and serial connections.

Figure 3
Direct modem and serial connections
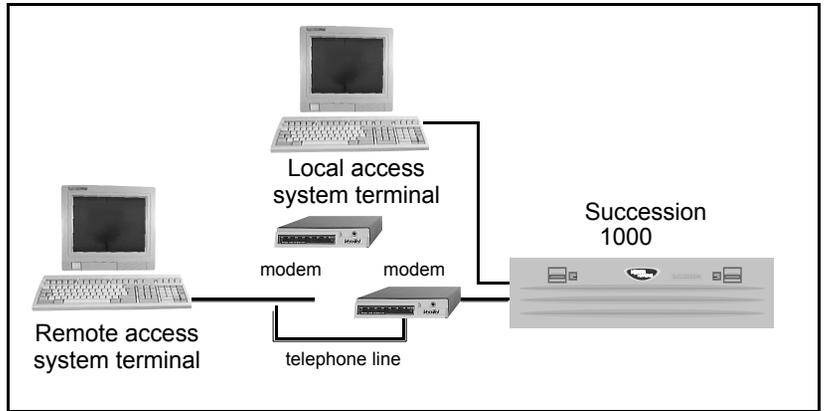
Local and remote access

Input/output 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 TLAN or ELAN network. Strictly-local access is over a serial cable connected directly to the component in question.

A device located within 50 feet of the central control unit is a local device and connects directly to an SDI card. A device located more than 50 feet from the central control unit is a remote device and must be connected to the SDI card through modems and a telephone line.

Figure 4
Local and remote devices

Succession 1000

Fault Reporting

Overlays

Overlay Sup.

CPU Bus

I/O Cards

RS-232

Modem

Modem

Local terminal/ console

Printer

Remote console

553-6304
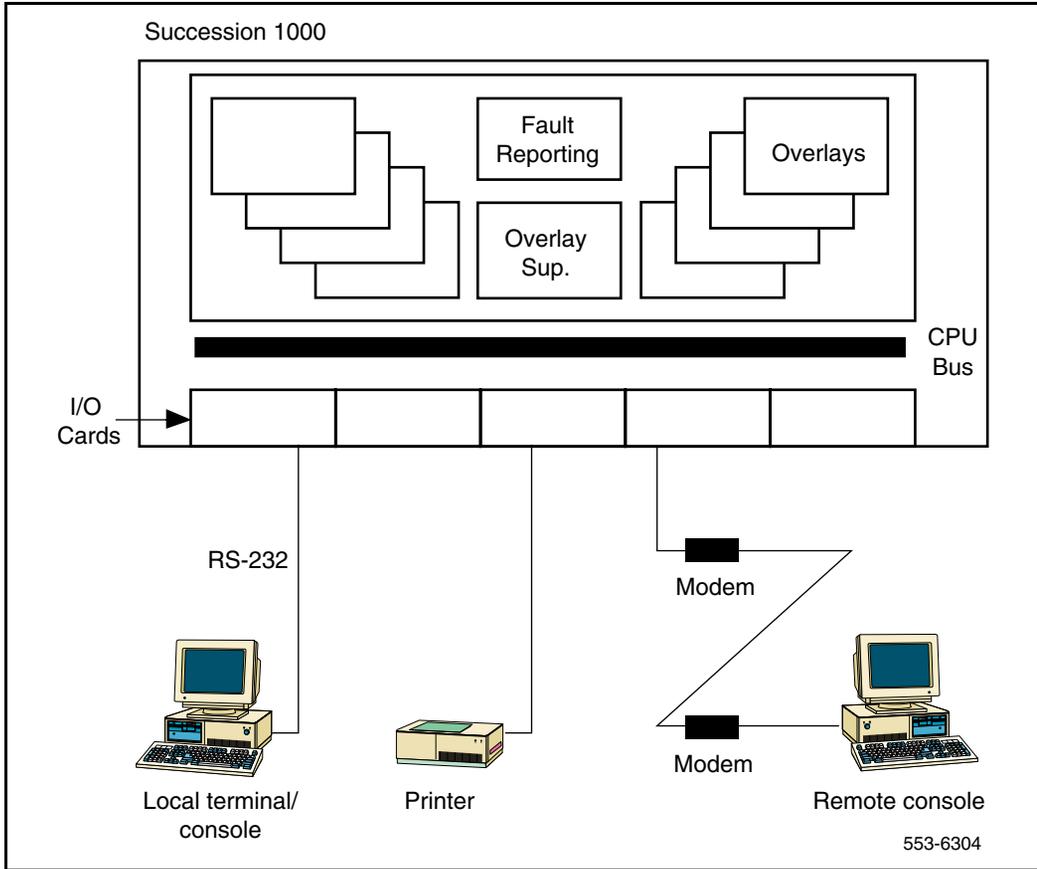
Local serial connections

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

Call Server

To access the Call Server, a Media Gateway, or H.323 WAN Gateway over a serial connection, consult "Communicating with the system" in the *Software Input/Output: Administration* (553-3001-311).

Alternatively, see "Access through the system terminal" in *Large System: Maintenance* (553-3021-500).

Signaling Server

To access the Signaling Server over a serial connection, consult "Connect and power up the Signaling Server" in *Succession 1000 System: Upgrade Procedures* (553-3031-258) and *Succession 1000 System: Installation and Configuration* (553-3031-210). The CLI is intended for advanced maintenance.

Voice Gateway Media Card

To access the Voice Gateway Media Card interface over a serial connection, consult "Voice Gateway Media Card ELAN and TLAN interfaces" in the *IP Line: Description, Installation, and Operation* (553-3001-365) guide. All management interfaces of the Voice Gateway Media Card are described and implemented in the *IP Line: Description, Installation, and Operation* (553-3001-365) guide.

Circuit cards

Each circuit card is described in the *Circuit Card: Description and Installation* (553-3001-211). If the hardware supports a serial interface, it is indicated in the guide. Documents specific to some circuit cards can apply.

Remote serial access

Call Server

The Call Server supports modem connections for serial maintenance terminal access or to establish a Point to Point Protocol (PPP, a protocol for communication between two computers using a serial interface) link for IP communication. See the "System terminals setup and connections" chapter of *Succession 1000 System: Installation and Configuration* (553-3031-210).

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* (553-3001-511).

Signaling Server

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

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

You can connect a modem to the Signaling Server and dial into it. Once connected you can use the Signaling Server CLI. You can also initiate a PPP session which would then enable you to access the Element Manager web page on your browser. From there, you can Telnet to the Voice Gateway Media Cards.

However, if the Signaling Server is experiencing a problem, and you need to connect remotely as part of a troubleshooting scenario, then the above connection cannot work. In anticipation of this scenario, you can connect multiple modems to the various serial ports of the Signaling Server, Voice Gateway Media Cards, Call Server and Media Gateway. In this way you can dial into the modem of the portion of the system you need to look at.

This approach for each system component is not practical or cost effective, as it requires the site to use multiple modems with multiple phone lines. Therefore, a better option is to use the 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

connection by the remote system administrator. It also includes an Ethernet interface which can enable a remote system administrator to Telnet to the device, and from there, telnet or rlogin to the various system components.

You can install a modem router on the system to facilitate remote management of components. Details are in "Appendix B: RM356 modem router" of *IP Line: Description, Installation, and Operation* (553-3001-365).

You can also install a terminal server, which is similar to a modem router, but with eight to twelve RS-232 serial ports that are cabled to individual components.

Maintenance connectivity for distributed components (not co-located) can require full 9-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, connect it to the network as described in "System Connections" in *Succession 1000 System: Installation and Configuration* (553-3031-210). The data network connection is through a Layer 2 switch on the network, which is also described in the "System Connections" section.

Closely associated with all data and management connectivity is the administrator's concern for security. 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 outlined in "Security" on page 81. If possible, use an access list on the routers, so that only certain users or ports are permitted into the ELAN, TLAN, or both.

Because system login authentication is always an aspect of security, refer to "Security" on page 81 for pertinent information.

Element Manager workstation

Element Manager is available through the Signaling Server ELAN or TLAN interface. For more information about ELAN and TLAN, see the *Succession 1000 System: Overview* (553-3031-010).

The management workstation can either be on the ELAN or TLAN, or have access to the ELAN or TLAN (for example, through a router or a switch on the customer data network). For more information about switch connections, see the *Data Networking for Voice over IP* (553-3001-160).

Optivity Telephony Manager windows workstation

The workstation for OTM must be on the ELAN or customer data network. OTM needs ELAN connectivity.

For information on using a modem with a remote OTM workstation, see "Add a V.24 serial connection" in *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331).

The *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331) guide contains a network configuration and connectivity description in the chapter "Overview of Optivity Telephony Manager". Everything pertinent to installing OTM on a workstation is included in *Optivity Telephony Manager: Installation and Configuration* (553-3001-230). See the "Determining the OTM PC IP address" section in the document. Also see "Connectivity through OTM" in the *Optivity Telephony Manager: System Administration* (553-3001-330).

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 left disabled and a system message is issued. A technician must then manually enable the port.

Point-to-Point access

The system has Ethernet ports and supports TCP\IP. Point-to-Point Protocol (PPP) is an asynchronous implementation of the standard data link level Point-to-Point Protocol included in the Internet protocol suite. This function

provides a common network interface for applications written to use the TCP/IP protocol stack for remote system access.

Operating parameters

Although one of the features of PPP is to support different network layer protocols, in the system client-server environments, only TCP/IP protocol is supported. This limitation does not alter the standard PPP implementation in any way or form to prevent supporting other protocol stacks in the future.

Though the PPP protocol is designed to support both synchronous and asynchronous data communications, only asynchronous data links are supported. The availability of a synchronous link depends on the driver for VxWorks and the type of SDI port that will be available for synchronous communications.

Only one active PPP link can be established at a given time to minimize the impact to the 68000 series CPU and memory usage by the amount of networking traffic from PPP and Ethernet.

Because of the different 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. Since the system always sets the most significant bit (8th bit) to "1", the receiving terminal must reset its terminal to mask off the 8th bit when communicating to system overlays.

System components

The system access and networking components include the existing system overlay and the VxWorks OS interface.Three types of remote connections are supported:

- Normal SDI interface to system overlays (current)

- Normal SDI with SLIP session through PDT (current for field support only)

- Normal SDI with PPP stack under VxWorks

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

Description

Point-to-Point Protocol provides a standard encapsulation scheme to transmit IP datagrams over a serial link. The advantage of adapting such a 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 for establishing PPP links on the type of SDI hardware supported systems.

SDI ports

For asynchronous PPP links, any physical SDI port configured on the 68000 series system with USER type MTC and/or SCH is supported. PPP is designed to provide the communication interface to the system application to perform administration and maintenance tasks. Therefore, the system SDI port used for the PPP link must be configured to MTC and/or SCH. Other USER types associated with MTC or SCH are considered valid SDI ports for a PPP link.

Port communication parameters

PPP protocol is designed to work in full duplex communications 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

- 8 Data bits, 1 Stop bit

- No parity

- Transmission mode set to DTE

- Standard RS-232C Interface

The SDI port should always be set to 8 data bits. For applications that need to set up an active TTY session through the same serial connection, the terminal emulation program should be set to ignore the 8th bit to avoid experiencing garbage characters on the terminal screen when accessing the system overlay.

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

Modem set up

Before a modem is connected to the system serial port, the modem must be configured correctly with an external terminal. Modem configuration should be saved in the modem's internal battery-backed memory to protect against power failure.

PPP link establishment

The implementations of PPP links over the system PBX require special treatments to work under the system operating systems. In a UNIX environment, PPP links require a dedicated serial interface. It is required to SHARE the MD1 SDI port.

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 TTY port must be connected to system input or the overlay supervisor directly (idle state) when the serial link is established. After the technician establishes the physical serial connection to the system, the PPP link can be invoked by issuing the pppBegin command. The pppBegin loads the PPP protocol and starts up the PPP Link Control Protocol (LCP, establish state). Once the LCP is established, the Networking Control Protocol (NCP) will be established for TCP/IP running on VxWorks (operation state). Should the LCP fail, the PPP link will be disabled and return control to the overlay supervisor (idle state). This login process can be automated by using a script file running on the remote access station.

Out-Bound PPP link establishment

Once the connection is made, the software will start up the PPP handshaking process (pppBegin) and establish LCP, PAP, and NCP as required.

PPP link termination

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

PPP link Access Log

The PPP link connection log records all the previous PPP links activities as 68000 series messages. This RPT log file is maintained for system logging purposes only, and can only be read from the PDT shell with the RPT commands.

Operation

System set up 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 1P layer must be configured correctly in LD 117.

- A valid operational TTY port must be available.

- A PPP configuration file must exist which can be configured in LD 117.

- Modem connections must be set up and an active connection established.

Configuring the network

Connecting the system core directly to a customer's LAN can cause some serious problems, such as broadcast packets, when the system core is too busy handling the data network traffic. A direct LAN connection provides access

to all the workstations on the LAN. With the right name and password, a user can access system core data through the login and/or FTP connection.

To protect the system core from LAN traffic and unauthorized access, an external router is recommended to shield the system core from the customer LAN and to block unauthorized access. Customers need to understand the performance impact and potential problems that can occur when the system core is connected to a LAN directly.

Before the TCP/IP network can be used, the system must be configured properly. The configuration consists of setting up various network database files and system start-up files. For a system PBX under the VxWorks operating system, the following areas must be configured in LD 117 based on the customer's data network requirements:

- The system name and IP address (primary and secondary IP addresses for dual IOPs).

- VxWorks Boot Parameter files

- The network host(s), default router, and subnet mask

If the system switch is connected to a customer's LAN, the above IP network configuration is not needed; the factory default setting is used instead.

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, and others cannot be used for PPP links. The port communication parameters must be validated by a technician before the port can be enabled for service; the PPP software cannot change the SDI port communication parameters configured in LD 117.

Due to the overhead of network traffic, set the SDI port baud rate at 9600bps 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 should be running. Depending on the PPP implementation, the format of the configuration will be different from one implementation to another.

Modem set up 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, it is impossible for the software driver to detect the baud rate at which the modem is established. As a result, the baud rate between the SDI port and the modem must be fixed.

A high-speed modem with fixed/variable speed DTE interface is strongly recommended. This allows the baud rate between the SDI port and the modem to be set higher than the actual link rate, enabling greater efficiency and throughput.

Operating parameters

Sysload

The active TTY port running a PPP session will be terminated when sysload occurs. The physical TTY port may be interrupted due to the sysload; the TTY port should remain enabled after the sysload. The PPP links must be re-established after the system sysload.

System INIT

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

PPP under remote access environments

When running applications to access the system remotely, a PPP link is used to interface to the remote application on the system core. If the remote OS 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 may get lost in the UART's receive buffer.

When such 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 will work if the remote access system is not under heavy load.

For a high speed PPP link (9600bps or above), the 16550 UART is recommended.

Ns26550 will ensure a reliable high speed serial link in a Microsoft Windows environment. The 8250 or 16450 UART will 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 do not have enough 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

Since 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/replacing the modem will not re-establish the PPP links.

Service change

The following table lists the commands associated with a service change.

LD 117 – Service change (Part 1 of 2)

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

LD 117 – Service change (Part 2 of 2)

Prompt	Response	Description
=>	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
=>	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	Re-build INDET.DB and re-number 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 should be configured to match the customer's data network requirements.

System Core without LAN access

There is no configuration required if the core is not connected to the customer's LAN. Only Nortel Networks applications are allowed access to the PPP and Ethernet.

System Core with LAN access

For customers who want to connect the system PBX to their LAN, an IP gateway or router is recommended 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. Network connection is only allowed by Nortel Networks applications.

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

Perform the following actions:

- Obtain the system core Internet Address

- Obtain valid IP names and addresses from the customer's network administrator.

- Use LD 117 to change the system default IP addresses to the new IP addresses. This includes the active and inactive Ethernet interface addresses and local and/or remote PPP interface addresses.

- For duel CPU setup, obtain two valid Ethernet interface IP addresses.

- Configure the subnet mask.

- Obtain the valid subnet mask from network administrator.

- Use CHG MASK in LD 117 to change the subnet mask for Ethernet interfaces.

- Obtain Network host names and addresses.

- Identify the host names and addresses in the data network.

- Add these host names and addresses through LD 117 "NEW HOST."

- Make sure the gateway or router is included in the host table.

- Obtain network routing information

In order 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 form the network/LAN administrator.

Perform the following actions:

- Obtain valid gateway/router and the network addresses.

- Use LD 117 'NEW ROUT" to add the network and gateway addresses.

- Verify that the gateway address is the host table.

- PPP: run time parameters

    — 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.

    — Configure the idle timer in LD 117 with 'CHG PTM nnn".

Diagnostic and maintenance programs

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

Fault clearance

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

- transmission
- connection
- system related faults

Transmission Faults

Due to the characteristics of asynchronous communications, data transmitting over the serial interface may 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 try to reconnect it with a new connection at a lower baud rate.

Connection faults

The connection fault is caused by either a hardware failure or the link carrier becoming 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 may still be up so that the technician should 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 go 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 disconnect and causes the PPP stack to close down. When such a condition occurs, re-establish the physical link and start up the PPP link again.

Security

Security for establishing PPP links requires the same login name and password process imposed by the system. Also, once the PPP link is established, the application residing on the system can provide additional security measurements if needed. Services provided by network OS, such as Telnet and rlogin, can be provided by the host machine. Current system security access to LAPW is supported in LD 117.

Unauthorized access to data

For the network services provided by VxWorks OS, some of the services may allow unauthorized access to system data. Table 3 lists the services available.

Table 3
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 during the process start ups. 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 needs to 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, TCP) is a fixed number of bytes for each data frame. The only part that can be improved is the re-transmission rate. A quality modem and line connection reduces the re-transmission rate, and a smaller data frame size improves performance.

Current system serial I/O will generate 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. 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 (IOP) 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) support Ethernet. Therefore, they can be connected to the system core by the Ethernet connection in the Customer LAN (CLAN) environment.

Operating parameters

The system is accessed from the industry standard Ethernet connection with the rate of transmission of 10 Mbits/second.

The use of Ethernet connection is restricted to Nortel Networks-managed products.

Affected components

Table 4
Affected Overlays

Affected Overlay	Changes
LD 43	New data included in data dump
LD 117	Commands are added to allow the user to configure and print the host names, and IP addresses.
LD 137	New ENL, DIS and STAT ELNK commands for enabling, disabling and checking the status of the Ethernet link.

Network address

Ethernet address

An Ethernet address is a 48-bit long address. It is a unique physical address assigned to the Ethernet controller equipped in the I/O Processor (IOP).

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 sets both IOPs to use only one Ethernet address for communications over the link.

IP address

An IP address is a 4-byte long address configured manually by the user. The IP address is also called the Internet address. Every IP address is associated with a host name.

On a redundant system, two IP addresses and host names must be specified: Primary and Secondary. Normally, the Primary IP Address (PIPA) is always the address 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 will be backed up to the floppy disk. When the customer performs a database restore, this file also gets 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 Ethernet address. In order to communicate over the Ethernet link, the IP address must be configured as well. Because the IP configuration is not fully implemented, the system has limited communication over the Ethernet link.

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

Operating parameters

Administration of IP addresses and maintenance of the LANCE can only be 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

This 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" on .

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 defaulted by the manufacture.

As part of the system Default Database, they are installed on the system through the existing Installation tool. The IP addresses are defaulted arbitrarily in the B class and the default host names are listed in Table 5.

Table 5
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. There are three operations that the core system must take into account:

1 **CPU switchover:** When this happens, the system core software will handle the network address resolution so that current connections over Ethernet should 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, hardware-sanity watchdog-timer-time-out.

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

    — Hardware (forced) switchover by the technician by turning the switch on the CP card to the maintenance position.

2 **CPU split:** When this happens, the system core software will handle 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 system in split mode by a technician.

3 **CPU redundancy:** When the system is redundant, the system core software will handle the network address resolution by setting the active CPU side so that it can communicate over the LAN. At this point, there is no communication with the inactive CPU side. This is a single Ethernet connection. 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 the system in the redundancy mode by a technician

Table 6 summarizes the possible states of a redundant system and the state of the Ethernet connection being used.

Table 6
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

Since the LANCE is equipped on the IOP card, changing the state of the IOP will have an effect on the LANCE. The state of the IOP is controlled by the following commands in LD 137:

• Disabling the active IOP by the command 'DIS IOP'. When this command is executed, the LANCE is disabled and becomes inaccessible.

- Enabling the active IOP by the command 'ENL IOP'. When this command is executed, the LANCE is enabled and becomes accessible.

- Checking the status of the active IOP by the command 'STAT IOP'. The status of LANCE is also checked. The Disable or Enable state is printed.

- Checking the status of both IOPs and Core Module Disk Units (CMDU) by the command 'STAT'. The status of both LANCEs (both CPU sides) are checked. If the status of LANCE is disabled, an Out-Of-Service (OOS) message is printed to indicate the reason.

The state of the IOP also can be changed by toggling the Enable/Disable switch on the card's faceplate:

- Disable the active IOP card by turning the switch to 'Dis' position. The LANCE will be disabled.

- Enable the active IOP card by turing the switch to 'Enb' position. The LANCE will be enabled.

- LANCE also is affected by the action of the user.

  — Remove the IOP card while the card is enabled and running. When the IOP card is re-inserted back into the slot, after reset logic of IOP passes, LANCE is re-enabled and accessible.

IOP power-up reset

When the IOP card is powered up, a self-test on the sub-components 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 will determine 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 time-outs will be handled by the ROM-based Exception handler. This handler will flash a HEX code in the case of a problem.

IOP hex display message

A hex code indication is displayed on the faceplate when LANCE fails the IOP Power-up self-test.

Abnormal operation

There are three types of errors related to the Ethernet link as described below:

*   **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.

A reset of the LANCE is necessary when one of the following conditions occur:

*   LANCE's memory response failure error

*   Buffer error

There is an attempt to switch CPUs in case of failure to reset the LANCE.

Service change

LD 117

The administration of the host names and IP address are done in LD 117. Table 7 on page 61 illustrates how to change the host name and IP address for the Primary and Secondary CPU side. Refer to "Direct Gateway Access" on page 75.

Ethernet configuration

Table 7 shows the prompt sequence and responses for configuring the Ethernet link in LD 117.

Table 7
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, a system warmset is needed to use this address.

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 should not be a digit.

Supported Host Name characters

For the Host Name, the system prints an error message if the user configures a name that is not supported. A valid name is a text string which includes the alphabet 'a' to 'z'., digit '0' to '9', underscore (_). Note that period is served as a delimiter between domain names. No space or tab characters are permitted. There is no distinction between upper case and lower case. The first character of the Host Name must be an alpha (a to z) character.

Ethernet printing

To print the Primary and Secondary IP addresses and host names from
LD 117, use the following commands:

Table 8
Ethernet printing

Prompt	Response	Description
=> PRT ELNI		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	System displays the Primary and Secondary addresses, and Host Names and addresses.

Ethernet Reset

To reset the Primary and Secondary IP addresses to the default, use the
following commands in LD 117.

Table 9
Ethernet reset

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

Traffic measurements and CDR outputs

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

Fault clearance procedure

The user can reset the Ethernet link directly by using LD 137 to disable and enable it. The system start-up process also resets the link before the communication can take place. The link reset action 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. An action can be taken.

Security

There is no additional security check for permission to administer the IP address in LD 117. All LD 117 users are allowed to administer the Ethernet.

The existing Multi-user feature for the system prevents more than one user from loading LD 117.

Hardware requirements

To have Ethernet operate in the ELAN, 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 requires a Video Display Terminal (VDT) or a Teletypewriter (TTY) 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 Table 10.

Table 10
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 Table 11.

Table 11
Device characteristics for the 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), 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, 62

- output only:

  > — RS-232-C compatible printer (PRT)

Logging in and out

Because the system supports multiple users, it provides security features to help ensure system integrity. One of these features requires that a system administrator complete a login sequence to begin an online session. For more information about security features, see "Security" on .

Logging in requires that the administrator enter the login command (LOGI) followed by a valid password. The system administrator can change passwords using LD 17. For added security, a login name can also be required.

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

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 "System messages" in
     Software Input/Output: System Messages (553-3001-411).

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

   • If the response is **>**, go to Step 4.

   • If the response is an error message, refer to "System messages" in
     Software Input/Output: System Messages (553-3001-411).

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 Step 4.

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

    LOGO <cr>

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

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 12 maps the keys on a system terminal keyboard to the telephone keys on a maintenance telephone.

Table 12
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
			0	0
		Space or #		#
		Return		##
Note: There is no Q or Z on a telephone.				

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 FFC. The Flexible Feature Code (FFC) is usually **30**. See "Flexible Feature Codes" in *Features and Services*

(553-3001-306)**.**

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. There are two choices:

- 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: ****

Background routines are then loaded automatically.

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. Because of how they are loaded, the programs are often referred to as overlays.

. The Flexible Feature Code (FFC) is usually 30. See "Flexible Feature Codes" in *Features and Services* (553-3001-306).

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

  Most other maintenance programs use a command/action/response format. The system administrator enters a command; the system performs the requested action and responds with the result. Table 13 on shows an example of a command recognized by several different maintenance programs.

Refer to *Software Input/Output: Administration* (553-3001-311) for the complete list of maintenance programs, as well as their prompt/response sequences.

Table 13
Maintenance program commands

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

Note: When the system administrator loads a maintenance program, it replaces any currently running background program except LD 44. Administrative routines (such as LDs 10 and 11) do not abort background routines.

Administration programs

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.

Once loaded, administration programs use a step-by-step prompt/response format. The program issues a prompt for input; the administrator enters the appropriate response through the keyboard, followed by the Return key. The Return key signals the end of each response. Table 14 on page 72 shows an example of how to use an administration program.

Table 14
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.
- 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 "System messages" in *Software Input/Output: Administration* (553-3001-311) 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 via 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 15.

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* (553-3001-311) for further detail.

Table 15
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
ALARM	Alarm filter

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.

The following table lists some data group mnemonics entered at the TYPE prompt in LD 22.

Table 16
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
ALARM	Print alarm filter tables

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* (553-3001-311).

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, floppies 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 into 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 17 shows some examples of the linked programs.

Table 17
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 is available supports on-line 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" on .

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 LDs 20, 21, and 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" on .

Using programs

Special characters

The characters shown in Table 18 have a special meaning to the software.

Table 18
Special characters and their meaning

Character	Meaning
**	Repeat current prompt
*	Return to REQ prompt
****	End the current program.
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" on page 165 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 19 lists the print programs and the type of data they can print.

Table 19
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
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 "Overlay characteristics" on .

For information on messages that may appear during program execution, see "System messages" on .

Software management

Contents

This section contains information on the following topics:

Introduction

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

Security

The system controls access to features and functions and provides audit trails of user sessions. Extensive system-wide security features help detect and prevent possible unauthorized access. For a comprehensive treatment of security topics, refer to *System Security Management* (553-3001-302).

For added security on remote connections, there are several options:

1 Use a dial-back modem with pre-assigned telephone numbers. The configuration of the modem and the dial-back feature is dependent on the make and model of the modem.

2 Dial into a Remote Access Server and authenticate your login on the network before using Telnet to access the component.

3 Dial into the modem on a workstation, and then use a remote control client such as PCAnywhere or Timbuktu to Telnet into the component.

Note: Remote control clients compromise security precautions. Security breaches can occur.

Refer to "Local and remote access" on for more information on connectivity.

To help control unauthorized access:

• Equipment should be stored in a physically secure area.

• Use perimeter security (such as router-based filtering or firewalls) to secure the ELAN.

• Remote access can be secured through Virtual Private Networks.

• Nortel Networks recommends using solid security practices that include password management and security audits.

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 passwords need to be changed using the "Basic system telephony configuration" chapter in *Succession 1000 System: Installation and Configuration* (553-3031-210).

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)**: These passwords provide general access to the system so that service personnel can perform administrative and maintenance tasks.

- **Level 2 passwords (PWD2 or admin2)**: These passwords provide restricted access to the System Configuration Record so that system administrators can change passwords and perform other tasks related to the system.

The system administrator (who must be logged in with PWD2) uses LD 17 PWD to enter or change passwords. The LNAME_OPTION in LD 17, which defaults to NO, must be set to YES to indicate that login names are required. An administrator 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 (Media Gateways, Signaling Servers, 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 default to their login name and password.

Each component of the system also has its own password to access the operating system or the command line 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 .

- 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 "Installing Signaling Server software" in *Succession 1000 System: Upgrade Procedures* (553-3031-258).

- The Gatekeeper has its own password. The default username is **gkadmin**. There is also guest access on the Gatekeeper. More information is in *IP Peer Networking* (553-3001-213).

- For Level 1, Level 2, and LAPW passwords in Element Manager, consult "Element Manager" on page 85. 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.

- For passwords on the Voice Gateway Media Card, consult "Change the default IPL> shell password" in *IP Line: Description, Installation, and Operation* (553-3001-365).

- For passwords on Internet Telephones (Station Control Password, Internet Telephone Installer's Password, Telephone Relocation password, Set Removal password), see *Branch Office* (553-3001-214).

Limited Access Passwords

With LAPWs, the system administrator can 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" on page 134.

In Element Manager, a user can create LAPWs, and users with Level 2 access can change Level 1 and Level 2 logins and passwords. See "Administration" in the *Succession 1000 Element Manager: System Administration* (553-3001-332) guide.

PDT password

For the Call Server and Media Gateway, the PDT shell, which is an expert-level tool, is password-protected. More information can be found in "Problem Determination Tool access information" in *System Security Management* (553-3001-302).

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.

With the Multi-User Login feature implemented, the system administrator can direct TTY session information to separate TTY log files. This is particularly useful to segregate system error messages from routine information messages. In addition, it lets the system administrator track sessions on a TTY where unusual login activities have occurred.

Signaling Server and Voice Gateway Media Cards

Report logs are available for errors and audit trails. See "Fault Management" on .

Element Manager

To log in to Element Manager, provide the same login name and password as would be used to log in to the Call Server. Authentication and permissions are determined by the Call Server. Password configuration (LAPW, Level 1, Level 2) is described in "IP telephony configuration using Element Manager" in *Succession 1000 System: Installation and Configuration* (553-3031-210)

and in the *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) guide.

The web server security flag enables the restriction of Element Manager access to hosts on the ELAN subnet. To enable or disable the web server security flag, use the Tools Menu from the Signaling Server Install Tool. Consult *Succession 1000 System: Installation and Configuration* (553-3031-210) for the procedure to invoke the Install Tool.

Report logs for errors and audit trails for the Call Server, Signaling Server and the Voice Gateway Media Cards are available through Element Manager. See "Fault Management" on .

Call Server

Logging in to Element Manager logs you into the Call Server. If you are logged in with a Level 2 password, you can change the passwords on the system. See "Configuration of data blocks and components" on .

The anti-password guessing feature, as implemented on the Call Server, is applicable to users of Element Manager. After three unsuccessful attempts to log in, access to Element Manager is denied for one hour.

Signaling Server

Security for Element Manager is implemented by RSA encryption on the web server. To ensure a secure login, Public Key Cryptography (PKC), based on the RSA algorithm, is used to encrypt the password prior to the login request being sent from the web client to the web server. With PKC, a public key is exchanged to the web client from the web server, without exposing any private keys. The public key is used for encrypting the data which is sent over from the web client to the server. The web server uses its own private key to decrypt the message.

The Web Server Configuration Parameter ensures that if no activity takes place within a configurable window, the user is logged out and must log back in again.

Note: The Gatekeeper administrator user name and password are the same as those for accessing the Gatekeeper shell. If you change the Gatekeeper Administrator user name or password, the shell user name and password are automatically changed.

If you forget the Signaling Server Administrator login, you can reset it using the Signaling Server Install Tool.

With administrator access to Element Manager on the Gatekeeper, you can change its password(s).

Element Manager also supports viewing the history file (see "History file" on page 85). For information on how to obtain the History file or other reports, see *Succession 1000 Element Manager: System Administration* (553-3001-332).

OTM

OTM can have multiple users, each having a set of access rights that determines what application they can access and with which privileges (read only or write). For more information, see "Security management" in *Optivity Telephony Manager: System Administration* (553-3001-330).

User groups

The OTM Administrator can determine what level of access the users in a particular User Group have to the features within OTM. User groups enable you to determine which sites and systems the members of the User Group are able to manage.

User Group Properties are separated into two major categories:

•   Navigator – Controls access to sites, systems, and applications for both the Windows Navigator and the Web Navigator.

•   Telephones – Controls access to telephones properties for Web Station Administration and Web Desktop Services.

User authentication

The following user authentication methods are available:

- Local OTM Server account

- Windows NT Domain account

- LDAP authentication

The OTM administrator can select any one of the three methods or a combination of the these methods to authenticate users on all OTM platforms: OTM Server, OTM Windows Client, and OTM Web Client.

For more information, see "Configuring Sites, Systems, and User accounts" in the *Optivity Telephony Manager: System Administration* (553-3001-330) guide.

Password encryption

All passwords transmitted or stored in the OTM database are encrypted.

Configuration of data blocks and components

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

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 20 presents the configuration tasks and the user interfaces that are available for these tasks.

Table 20
Configuration of data blocks (Part 1 of 5)

Activity or Datablock	Overlay	Element Manager	OTM 2.0
Time and Date	2	System Utility	Date and Time	No
Analog telephones	10	No	OTM Station Administration
Digital telephones	11	No	OTM Station Administration
Attendant Consoles	12	No	No
Digitone receivers, tone detection, multifrequency sender and receiver	13	No	No
Trunk Data Block	14	Configuration	Customer Explorer	Route Property Config	No

Table 20
Configuration of data blocks (Part 2 of 5)

Activity or Datablock	Overlay	Element Manager	OTM 2.0
Customer Data Block 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 ANI Configuration | Customer Explorer | Basic Configuration FCR Configuration | Flex. Code Restriction FTR Configuration | Customer Explorer | Feature options LDN Configuration | Customer Explorer | Listed Directory Number options NET Configuration | Customer Explorer | ISDN and ESN networking options NIT Configuration | Customer Explorer | Night Service options	No
Route Data Block	16	Configuration | Customer Explorer | Basic Configuration	No
Automatic Trunk Maintenance	16	No	No

Table 20
Configuration of data blocks (Part 3 of 5)

Activity or Datablock	Overlay	Element Manager	OTM 2.0
Configuration Record 1 -ADAN -ALARM -ATRN -CEQU -OVLY -PARM -PWD -VAS -ROLR/TOLR / APLR -HRLR / HTLR	17	Partial ADAN Configuration ǀ D-Channel CEQU Configuration ǀ Common equipment PWD Administration ǀ Password	-PWD OTM User Administration
Speed Call Group Call Pretranslation Special Service 16-Button DTMF Hotline	18	No	Partial OTM Speed Call List
Code Restriction	19	No	No
Automatic Call Distribution Management Reports Message Center	23	No	No
Direct Inward System Access	24	No	No
Group Do Not Disturb	26	No	No
ISDN Basic Rate Interface (BRI)	27	No	No
Route Selection for Automatic Number Identification	28	No	No
Memory Management	29	No	No

Table 20
Configuration of data blocks (Part 4 of 5)

Activity or Datablock	Overlay	Element Manager	OTM 2.0
New Flexible Code Restriction and Incoming Digit Conversion	49	Partial Configuration | Flex. Code Restriction Configuration | Incoming Digit Conversion	OTM ESN Analysis and Reporting Tool
Call Park and Modular Telephone Relocation	50	No	No
2.0 Mb/x Remote Peripheral Equipment	52	No	No
Flexible Tones and Cadences	56	No	No
Flexible Features Codes	57	No	No
Radio Paging	58	No	No
Digital Trunk Interface	73	Configuration | Digital Trunk Interface	
Digital Private Network Signaling System Link	74	No	No
Virtual Network Service	79	No	No
Set Designation Entry (ODAS)	84, 85	No	No
Electronic Switched Network 1	86	Network Numbering Plan | Call Server	OTM ESN Analysis and Reporting Tool
Electronic Switched Network 2	87	Network Numbering Plan | Call Server	OTM ESN Analysis and Reporting Tool

Table 20
Configuration of data blocks (Part 5 of 5)

Activity or Datablock	Overlay	Element Manager	OTM 2.0
Authorization Code	88	No	OTM Directory Services *
Electronic Switched Network 3	90	Network Numbering Plan	Call Server	OTM ESN Analysis and Reporting Tool
Multi-Tenant Service	93	No	No
Multifrequency Signaling	94	No	No
Call Party Name Display	95	No	OTM CPND Administration
Configuration Record 2	97	No	No
Ethernet and Alarms Management	117	Partial Configuration	Zone	No
*The Authorization Code is stored in the OTM Directory Services for billing purposes. It cannot be configured from this tool.			

Signaling Server

Table 21 provides a key to Signaling Server activities.

Table 21
Signaling Server configuration

Activity	Command Line Interface	Element Manager	OTM 2.0
Configuration parameters	Partial	GK Active DB Admin GK Standby DB Admin Configuration | IP telephony	OTM Site and System Administration Integrated link to Element Manager
Gatekeeper numbering plan	Partial	GK Active/Standby DB Admin | CDP Domains GK Active/Standby DB Admin | H323 Endpoints GK Active/Standby DB Admin | Numbering Plan Entries	OTM Site and System Administration Integrated link to Element Manager

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 *IP Line: Description, Installation, and Operation* (553-3001-365).

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 3.0 (IP telephony)

The parameters that are hosted on the Voice Gateway Media Cards and on the Signaling Server are configured using Element Manager (they are not

configured using OTM). When IP Line 3.0 is used with Meridian 1, the configuration is performed using OTM. All IP Line commands and interactions are documented in *IP Line: Description, Installation, and Operation* (553-3001-365).

IP Peer Networking / Gatekeeper

The IP Peer Networking parameters that exist on the Call Server and Voice Gateway Media Cards are configured using Element Manager. They are not configured by OTM. IP telephony parameters are described and implemented in *Succession 1000 System: Installation and Configuration* (553-3031-210). Gatekeeper parameters are described and implemented in the *IP Peer Networking* (553-3001-213).

OTM

The following sections describe some of OTM's configuration capabilities.

Station Administration

The Station Administration application (both Windows and web-based) helps administer databases that define end-user stations (telephones) on Succession 1000, Succession 1000M, and Meridian 1 systems. Station Administration allows you to add and edit the configuration of telephones.

Station Administration also manages Call Party Name Display (CPND) data. The List Manager component manages data for Speed Call, Group Call, and Group Hunt lists.

For more information, refer to "Station Administration" in *Optivity Telephony Manager: System Administration* (553-3001-330).

IP Line card configuration

The IP Line cards are required to be upgraded to IP Line 3.1. This upgrade requires OTM or the CLI, and the procedures are found in the *Succession 1000 System: Upgrade Procedures* (553-3031-258) and in the *IP Line: Description, Installation, and Operation* (553-3001-365) guides.

A Voice Gateway Media Cards is a Succession Media Card or ITG-P 24 port card running the IP Line 3.1 application. Voice Gateway Media Cards are

used in Succession 1000M, Succession 1000, and Meridian 1 product lines. Each system manages the Voice Gateway Media Cards differently: IP Line 3.1 requires OTM for management on Meridian 1 systems, and IP Line 3.1 requires Element Manager on Succession 1000 and Succession 1000M systems.

Internet Telephones

OTM provides the configuration and maintenance of IP Line cards for Internet Telephones. The configuration of Internet Telephones is accomplished through the Station Administration application in OTM. For more information, refer to IP Line: Description, Installation and Operation (553-3001-365).

802.11 Wireless

OTM is also used for the configuration and maintenance of the IP Trunk card for wireless service. For more information, refer to 802.11 Wireless IP Gateway for Meridian 1 (553-3001-206).

IP Trunks

OTM configures and maintains the IP Trunk card that resides in the IPE shelf of the system. The card appears to the switch as a trunk card with ISDN Signaling Link (ISL) and D-channel signaling. The card has a 10/100BaseT connection to carry packetized voice and fax calls over IP data networks, and can serve as a toll bypass to the traditional PSTN. For more information refer to IP Trunk: Description, Installation, and Operation (553-3001-363).

ESN configuration

The ESN Analysis and Reporting Tool (ESN ART) configures, analyzes, and manages large and complex ESN databases. ESN ART enables you to retrieve the ESN configuration from a system, and convert the overlay-based data into a database. Using the Windows user interface, you can easily view, modify, and print the data. The database can then be transmitted back to the system.

For more information, refer to "ESN Analysis and Reporting Tool" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Meridian DECT

The OTM DECT Management application is mandatory to implement DECT. It is described in *Meridian/Succession Companion DECT: Overview* (553-3601-103).

Fault Management

Command Line Interface

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

Call Server

All fault clearing procedures are in *Large System: Maintenance* (553-3021-500) according to system component. Both CLI and OTM procedures are documented.

Alarms status summaries are printed by LD 2. The alarms and exception filter summary printed by this overlay are discussed in *System Management* (553-3001-300) and *Software Input/Output: Maintenance* (553-3001-511).

Alarm monitoring and management

System alarms are based on various fault monitors and indicators. The category of the alarm – major, minor, or remote – indicates the severity of the system failure:

- A major alarm requires immediate action by the system administrator. It indicates a fault that seriously interferes with call processing.

- A minor alarm requires attention, but not necessarily immediate attention by the system administrator. It indicates the system hardware or software has detected a fault requiring attention.

- A remote alarm can require attention by the system administrator. 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 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* (553-3001-511) 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. 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, see "LED" in *Large System: Maintenance* (553-3021-500).

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 "HEX" in the *Software Input/Output: System Messages* (553-3001-411).

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 22 gives an example of the format for a system message.

Table 22
System message format

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* (553-3001-311) for a description of all maintenance commands, and the *Software Input/Output: System Messages* (553-3001-411) for the interpretation of all system messages.

System History File

The History File (see also "History file" on page 85) is a file to which the system writes messages, thus reducing the need for on-site TTY facilities. The contents of the file, which survive a sysload, are available for problem diagnosis and can be printed at any time. Printed History File messages are prefixed by a percent sign (%) to differentiate them from normal TTY printed output.

The LD 22 print routine supports View History File (VHST) for selectively viewing and/or printing System History File (and Traffic Log File) contents. VHST provides a comprehensive set of commands for this purpose.

If you have a printer connected to the system, each system message is printed as it is received. If you do not have a printer connected, you can use the History File to store a limited number of system messages in protected memory. The contents of the file can then be printed on demand using Print Routine 3 (LD 22).

The messages stored are specified on a system basis and can be one or more of the following types:

- customer service changes (CSC)

- maintenance messages (MTC)

- service changes (SCH)

- software errors (BUG)

- initialization and sysload messages (INI and SYS)

One History File can be specified per system. It is a circular file. When the file is full, the system "wraps" to the beginning of the file, overwriting the oldest entry.

TTY Log File

With the Multi-User Login feature enabled, the log files associated with system TTY terminals record messages relating to service changes, user invoked Maintenance operations, traffic (user requested reports through LD 2), CDR activity, software bugs, and so forth. Messages recorded in a TTY Log File are not written to the History File (see "History file" on).

System messages do not appear in this log, but they appear in the System History File. This file is lost upon sysload.

System Event List

With the Alarm Management feature, all processor-based system events are processed and logged into a disk-based System Event List (SEL). Events which are generated as a result of administration activities, such as SCH or ESN error messages, are not logged into the SEL. Events which are generated as a result of maintenance or system activities, like BUG and ERR error

messages, are logged into the SEL. Unlike the previous System History File, this SEL survives a sysload.

For more information on the disk-based System Event List, refer to LD 117 *Software Input/Output: Maintenance* (553-3001-511).

Signaling Server

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

Voice Gateway Media Cards

Voice Gateway Media Cards have faceplate displays that indicate their status. See "Hardware faceplate displays" on . Resident system reports exist on Voice Gateway Media Cards. For more information, see "Voice Gateway Media Card maintenance" in *IP Line: Description, Installation, and Operation* (553-3001-365).

The ITG/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 ITG 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, but does not support receiving traps and alarms.

However, Element Manager allows you to view the alarm and exception log histories and resident system reports for the Signaling Server, Voice Gateway Media Cards, and the Gatekeeper. For more information, see "History file" on . For more information on how to view faults and logs, see *Succession 1000 Element Manager: System Administration* (553-3001-332).

OTM

OTM has web and Windows applications to collect and filter alarms. It also manages errors at the level of each hardware component. OTM receives SNMP traps from systems and stores them in a circular log file on the OTM Server. The OTM Alarm Notification application monitors the incoming traps and notifies the appropriate people of important events and alarms. See "Alarm management" and "Maintenance applications" in *Optivity Telephony Manager: System Administration* (553-3001-330). OTM has the capability to forward alarms to a network management platform such as ONMS and HP OpenView.

Table 23 shows the supported functionality related to access and alarm management in OTM as it relates to other Nortel Networks products.

Table 23
Supported features (Part 1 of 2)

System	SNMP traps (Alarm Browser)	SNMP Traps (Alarm Notification)	Text alarms (DBA)	Forward to NMS (Alarm Browser & Alarm Notification)	Help (Alarm Browser & Alarm Notification)	Serial access via OTM	Telnet Access via OTM	GUI access via OTM	Web Access via OTM
Meridian 1 Succession 1000 Succession 1000M	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ITG	Yes	Yes	N/A	Some Issues *Note 1	Partial *Note 2	Yes	Yes	Yes	N/A
CallPilot 1.07, 2.0	Yes	Yes	N/A	Some Issues *Note 1	Partial *Note 2	N/A	N/A	Some Issues	N/A

Table 23
Supported features (Part 2 of 2)

System	SNMP traps (Alarm Browser)	SNMP Traps (Alarm Notification)	Text alarms (DBA)	Forward to NMS (Alarm Browser & Alarm Notification)	Help (Alarm Browser & Alarm Notification)	Serial access via OTM	Telnet Access via OTM	GUI access via OTM	Web Access via OTM
SCCS 4.0	Yes	Yes	N/A	Yes	Yes	N/A	N/A	No	N/A
OTM DECT Manager	Yes	Yes	N/A	Yes	No	Yes	Yes	Yes	Yes
MDECT Manager for Windows	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	N/A
MIRAN 2, 3	N/A	N/A	N/A	N/A	N/A	N/A	Yes	N/A	Yes
9150 Remote Office	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Some Issues	N/A
MICB 2, 3	N/A	N/A	N/A	N/A	N/A	N/A	Yes	N/A	Yes

Note:
1: Forwarding alarms requires writing scripting support and translation.
2: Help is available in Alarm Browser only.

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* (553-3001-311)).

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* (553-3001-350).

Element Manager

Element Manager does not support any billing applications.

OTM

CDR can be compared against the Corporate Directory in OTM for call origination and billing purposes. For information on CDR applications in OTM, refer to *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331).

The following sections provide a brief description of the telemanagement applications available for OTM.

Telecom Billing System

TBS is OTM's advanced cost allocation and billing application that:

• Collects call records from the system using defined communications and collection parameters.

- Allocates costs to the appropriate users, using multiple costing models over multi-level organizational hierarchies, and generates detail and summary reports outlining these costs. These reports detail the actual usage of the telephone system.

- Reports network utilization and system administration to manage a telecom network more effectively.

Consolidated Call Cost Reports

The Consolidated Call Cost Reports (CCCR) synchronizes the organization's information and calling activity from the individual OTM systems. First, use the Telecom Billing System to collect and cost the CDR data for each system. Then, using CCCR, perform the following actions:

- Combines data from the Corporate Directories in each OTM system and generates billing reports based on this consolidated data.

- Reports on calling activity across multiple systems on a single OTM server.

For more information on the TBS and CCCR, see their respective chapters in *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331).

Telecom Billing System Web Reporting

TBS Web Reporting is OTM's web based reporting application that:

- Generates reports containing data from TBS through an Intranet or Internet server. These reports provide information about organizational calling activities.

- Enables web-based viewing from any workstation with Intranet or Internet access to the OTM TBS Web Reporting server.

Refer to "Billing Reports" in *Optivity Telephony Manager: System Administration* (553-3001-330) (which describes the web service) for information on exporting CDR records for billing applications.

General Cost Allocation System

The General Cost Allocation System is OTM's generic billing application that:

- Assigns usage charges to appropriate individuals or departments within an organization.

- Imports bill information, identifies and logs departmental or user-specific spending characteristics, and generates meaningful reports summarizing these costs.

- Enables entering billing information that is used to allocate charges, such as those obtained from cellular calls or pagers, to relevant individuals or departments within organizations.

- Generates detail and summary reports including the billed products or services, associated costs and departments, or persons to be billed.

Consolidated Reporting System

The Consolidated Reporting System is OTM's telemanagement reporting application that:

- Generates reports for both the Telecom Billing System and the General Cost Allocation System from a single interface.

- Generates custom reports are that detail organizational and employee spending characteristics. Each report is broken down into subreports which detail usage costs for the Telecom Billing System and the General Cost Allocation System.

Call Tracking

Call Tracking is OTM's call monitor and alarm application that:

- Indicates trends and provide displays of unusual calls enabling adjustment of equipment and services.

- Monitors and displays information output from the system. It accumulates this data and provides the information in different formats in graphical displays.

- Provides alarm generating functions which can be set up to warn of unusual calling patterns.

These abilities can be configured to output different types of alarms including: visible and audible alarms on workstations; remote paging; and network reported alarms.

Performance monitoring

The performance-related tasks listed in Table 24 are available with Succession 1000 management.

Table 24
Traffic analysis

Component	Command Line Interface	Element Manager	OTM
Call Server and Media Gateway	LD 2	No	OTM Traffic Analysis
Signaling Server	Gatekeeper log files	Partial Live Gatekeeper | OMM	No
Voice Gateway Media Card	Operational Measurements reports	Partial System Status | IP telephony | OM RPT	OTM OM report

Maintenance activities on the Succession 1000 are discussed in *Succession 1000 System: Maintenance* (553-3031-500). Maintenance activities on the Voice Gateway Media Cards are discussed in *IP Line: Description, Installation, and Operation* (553-3001-365).

Command Line Interface

The following sections describe the Command Line Interface (CLI) performance monitoring activities.

Call Server

On the Call Server, LD 2 is the overlay in which you can set traffic report schedules, as described in *Software Input/Output: Administration* (553-3001-311).

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.

Voice Gateway Media Cards

The IP Line application supports operational measurements that can be obtained through the CLI. The operational measurements file contains counts of incoming and outgoing calls, call attempts, calls completed, and total holding time for voice and fax calls. For more information, see the *IP Line: Description, Installation, and Operation* (553-3001-365).

Element Manager

The following sections describe performance monitoring through Element Manager.

Signaling Server

The Element Manager web interface enables you to view the traffic level history through the Gatekeeper- and Signaling Server-specific performance monitoring. 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. For more information about endpoint activities, see the *IP Peer Networking* (553-3001-213).

Element Manager also enables you to perform the following Gatekeeper-specific performance monitoring functions:

*   *Monitor the state of endpoint registrations*. This shows 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*. 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*. In every Admission Request (ARQ), the ARQ administrator provides a bandwidth field. The Gatekeeper logs the total bandwidth requested on an hourly basis.

- *View the alarm and exception log histories for the Gatekeeper and Signaling Server*. See "Fault Management" on .

With guest access to Element Manager on the Gatekeeper, you can view output from the performance monitoring functions. For more information about the Gatekeeper and Element Manager, see the *IP Peer Networking* (553-3001-213) and *Succession 1000 Element Manager: System Administration* (553-3001-332) guides.

Voice Gateway Media Card

Element Manager supports the display for IP telephony component status. For more information, see the *IP Line: Description, Installation, and Operation* (553-3001-365).

Operational Measurement reports are on a per-card basis, where you can select the eight most recently-developed reports.

OTM

OTM offers a Traffic Analysis application supporting the traffic information for the Call Server. ITG/IP Line and ITG/IP Trunk Operational Measurement data can also be collected using OTM ITG application.

Call Server

Traffic Analysis performs the following functions:

- Collects traffic data from a specific Succession 1000 system

- Maintains a database of collected traffic data

- Defines report and graph parameters

- Generates reports to extract significant information from raw traffic data, such as trunk usage, peak periods, process loads and junctor and loop traffic

See the "Traffic Analysis" chapter in *Optivity Telephony Manager: System Administration* (553-3001-330).

ITG Operational Measurement reports

The OTM IP Trunk and IP Line 3.1 application, enables you to retrieve operational measurement reports generated by Succession IP Peer (virtual trunks) and IP Line features. For more information, see "IP Line Operational Measurement report scheduling and generation" in *IP Line: Description, Installation, and Operation* (553-3001-365).

Utilities

Command Line Interface

The following sections describe the Command Line Interface (CLI) utilities.

Call Server

Utilities on the Call Server and Media Gateway CLI can be found in Input/Output guides *Software Input/Output: Administration* (553-3001-311) and *Software Input/Output: Maintenance* (553-3001-511).

Equipment Data Dump (EDD) is performed using LD 43 on the Call Server. It backs up and synchronizes copies of the customer database to its associated Media Gateways. Database backup and restore is performed using the Utilities menu from the Software Installation Program. For more information, consult the *Succession 1000 System: Installation and Configuration* (553-3031-210) and the *Succession 1000 System: Upgrade Procedures* (553-3031-258).

The system date and time can be set during system installation, or configured using LD 2. This task is discussed in "Configuration of data blocks and components" on .

Corporate Directory is available from LD 11.

OTM workstation

The Access Server provides a CLI for remote access to the OTM server. A modem or a direct serial connection can dial in from a remote terminal connection to different sites and systems as configured in Virtual Terminal Service. The workstation running OTM can provide a single point of access to LAN and serial ports. See "Server access" on .

From a workstation other than the OTM Server, HyperTerminal or an equivalent Telnet application dials into CLI on the OTM Server.

See "Access Server" in *Optivity Telephony Manager: System Administration* (553-3001-330).

The System Terminal application on OTM is a pass-through to the Succession 1000 CLI. See "System Terminal" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Element Manager

All Element Manager utilities are described in the *Succession 1000 Element Manager: System Administration* (553-3001-332) guide.

Call Server Backup

The Call Server Backup function invokes a data dump and writes the Call Server data to the primary and internal backup drives. The Backup function performs the same task as the 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.

System Date & Time

The System Date & Time function enables modification of the system's current time and date using Element Manager. The System Date & Time function performs the same task as the CLI STAD command in LD 02.

Centralized file upload

The Centralized file upload function enables uploading and storing software, firmware, and patches on the Signaling Server. These files are downloaded to IP telephones and other IP telephony components using the functions available under the Software Upgrades and Patching branches of the navigation tree.

OTM

The following sections describe OTM utilities.

LDAP access

LDAP server refers to an external corporate directory that is Lightweight Directory Access Protocol (LDAP)-compliant. The LDAP Synchronization utility synchronizes user data between the OTM Directory, Station Administration database, and the LDAP directory. LDAP Synchronization is a scheduled activity that runs in the background, or can be performed manually. OTM supports four types of LDAP servers:

- Netscape Directory

- Microsoft Exchange Server

- Novell NDS

- Active Directory

LDAP synchronizations are set up and scheduled from the Utilities menu. When a user is added to the LDAP-compliant external corporate directory, the user is manually entered to the OTM directory for the appropriate system.

See "LDAP Synchronization" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Corporate Directory

OTM's Corporate Directory defines and generates reports of station data associated with a Terminal Number (TN). A prime use of the Corporate Directory functionality is to generate the set directory to be used for M3900 and Internet Telephone. In addition, reports can be generated with numerous

data fields, including the name, extension, location, and department. This can be used to generate a hard-copy directory listing.

See "Corporate Directory" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Inventory management

All telemanagement applications are described in "Optivity Telephony Manager" on . See the *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331) guide.

Station Administration allows you to run an equipment inventory report. See "Running Reports" in *Optivity Telephony Manager: System Administration* (553-3001-330).

For more about Inventory Reporting, see "Windows-based and web-based maintenance" on .

Data buffering

The OTM Data Buffering and Access (DBA) application provides a Windows interface to start a live data buffering session and define the session properties for collecting data from a system. A network or PPP connection enables collection of CDR and Traffic data. A serial connection enables collection of ASCII data only.

See "Data Buffering and Access" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Server access

The Virtual Terminal Service provides the connection between a browser and a device or system. The OTM Web Navigator is launched from a Web browser, such as Internet Explorer or Netscape Navigator, and selected to view a system or other device.

OTM's Web System Terminal window accesses systems and devices from within a Web browser, without referring to IP addresses, serial port settings, or URLs.

See "Connectivity through OTM" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Terminal emulation

System Terminal provides a terminal emulation capability using the VT220 application.

The VT220 terminal emulation application models the VT100/220/320 series of terminals to set up communications between workstations and the system. The VT220 connects to the system using a serial, PPP (point to point protocol), or Ethernet connection. It supports the transfer of ASCII data during a communications session and provides normal TTY and VT220 access to overlays that are not supported by the OTM applications.

See "System Terminal" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Database backup and restore

The OTM Data Buffering and Access (DBA) application provides scheduling of a single or routine backup of the system's database files.

A schedule can be implemented for the retrieval of buffered CDR and Traffic data from the system to the workstation.

See "Backup and Restore" in *Optivity Telephony Manager: System Administration* (553-3001-330).

System Monitor

The System Monitor utility enables the following:

- turn a system alarm on or off and define the conditions (where, when, and what type of alarm) for sending alarm messages

- enable the System Monitor to automatically start when Navigator starts

- view the virtual, physical, and total memory available

- view the total CPU usage information

- view the processes currently running on the system

- view the applications currently running on the system

- view the performance of the Windows NT server

- "ping" another machine to test network connections

See "System Monitor" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Scheduler

The Scheduler schedules an Optivity Telephony Manager activity (or any Windows application activity) for processing at a later date and time. Scheduler defines the intervals to run the activity. If there are multiple tasks in a job, tasks are assigned in a sequential order using the queue function.

See "Scheduler" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Import and Export

The Import and Export utilities are used to import data from and export data to the Optivity Telephony Manager (OTM) database files. These tools enable the sharing of data between the OTM databases and other applications.

See "Import and Export utilities" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Compact and Repair

The Compact and Repair utility compacts or repairs OTM database files for specific sites and systems. This utility compacts or repairs any Microsoft Access format database files of the same version as OTM (For example, Microsoft Access 97).

See "Database Compact/Repair utility" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Client Utility

The Client Utility updates the OTM database when the host name or IP address of an OTM Client machine has changed. The Client Utility

removes an OTM Client machine from the OTM database when re-assigning the Client license to a new OTM Client.

See "Client Utility" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Equipment Data Dump

OTM's Equipment Data Dump (EDD) is a critical database update operation on the system. This operation dumps (saves) modified data from the switch's resident memory to database files on the switch's hard disk. These database files contain the active configuration information for telephone-system terminals and users.

See "Equipment Data Dump" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Maintenance

Table 25 represents a non-exhaustive list of maintenance tasks that can be performed with Succession 1000 management.

Table 25
Maintenance activities (Part 1 of 2)

System component	Activity	Command Line Interface	Element Manager	OTM
Call Server	Status	See Table 26 on page 118.	System Status | Call Server	OTM Maintenance Windows / Web
	Patches	Yes	Patching | Call Server Patching | Media Gateway	No

Table 25
Maintenance activities (Part 2 of 2)

System component	Activity	Command Line Interface	Element Manager	OTM
Signaling Server	Status	Partial	System Status | IP telephony	No
	Backup/Restore		GK Active DB Admin | Database Backup	
	Software download		Software Upgrade | File Upload	
	Patches download and activation		Patching | IP telephony	
Voice Gateway Media Card	Status / Error messages	Partial	System Status | IP telephony | Sys Log	OTM Maintenance Windows / Web
	Patches download and activation	Partial	Patching | IP telephony	No (OTM supports Large System IP Line cards)
	Loadware and firmware versions and upload	Partial	Software version | IP telephony Software Upgrade | File Upload	OTM IP Line application
	IP Line and Internet Telephone maintenance and diagnostics	LD 32—See Table 26 on page 118.		

For maintenance activities on the Succession 1000 system, see
Succession 1000 System: Maintenance (553-3031-500).

For maintenance commands specifically available through Element Manager, refer to *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232).

Call Server activities

The datablocks and activities listed in Table 26 are available on the Call Server.

Table 26
Maintenance overlays (Part 1 of 3)

Activity or Datablock	Command Line Interface	Element Manager	OTM
Template Audit	LD 1	No	
Network and Signaling Diagnostic	LD 30	No	OTM Maintenance Windows / Web
Telephone and Attendant Console Diagnostic	LD 31	No	No
Network and Peripheral Equipment Diagnostic	LD 32	System Status | Call Server | Network and Peripheral Equipment Diagnostic	OTM Maintenance Windows / Web
Peripheral Equipment Diagnostic for 1.5 Mb/s RPE and Fibre Remote IPE	LD 33	No	OTM Maintenance Windows / Web
Tone and Digit Switch and Digitone Receiver Diagnostic	LD 34	No	OTM Maintenance Windows / Web
Trunk Diagnostic	LD 36	System Status | Call Server | Trunk Diagnostic	No
Input/Output Diagnostic	LD 37	No	No
Conference Circuit Diagnostic	LD 38	No	No

Table 26
Maintenance overlays (Part 2 of 3)

Activity or Datablock	Command Line Interface	Element Manager	OTM
Intergroup Switch and System Diagnostic	LD 39	No	OTM Maintenance Windows / Web
Call Detail Recording Diagnostic	LD 40 LD 42	No	TBS Event Log Viewer
Equipment data dump Database backup and restore	LD 43	System Utility | Backup System Utility | Restore	OTM Backup and restore
Software Audit	LD 44	No	No
Background Signaling and Switching Diagnostic	LD 45	No	No
Multifrequency Sender Diagnostic for Automatic Number Identification	LD 46	No	OTM Windows Maintenance
Link Diagnostic	LD 48	No	No
Intercept Computer Update	LD 51	No	OTM Windows Maintenance
2.0 Mb/s Remote Peripheral Equipment Diagnostic	LD 53	No	OTM Maintenance Windows / Web
Multifrequency Signaling Diagnostic	LD 54	No	OTM Windows Maintenance
Digital Trunk Interface and Primary Rate Interface Diagnostic	LD 60	System Status | Call Server | Digital Trunk Card Diagnostic	OTM Maintenance Windows / Web
Message Waiting Lamps Reset	LD 61	No	No

Table 26
Maintenance overlays (Part 3 of 3)

Activity or Datablock	Command Line Interface	Element Manager	OTM
1.5 Mbps Remote Peripheral Equipment Local End Diagnostic	LD 62	No	OTM Maintenance Windows / Web
Conversion	LD 66	No	No
Digital Trunk Maintenance	LD 75	No	OTM Maintenance Windows / Web
Manual Print	LD 77	No	No
Call Trace	LD 80	No	OTM Call Tracking
Automatic Trunk Maintenance	LD 92	No	OTM Maintenance Windows / Web
D-Channel Diagnostic	LD 96	System Status	Call Server	D-Channel Diagnostic	OTM Maintenance Windows / Web
Ethernet and Alarm Management	LD 117	No	No
Core Common Equipment Diagnostic	LD 135	No	OTM Maintenance Windows / Web
Core Input / Output Diagnostic	LD 137	No	OTM Maintenance Windows / Web
Customer Configuration Backup and Restore	LD 143	No	OTM Backup and restore

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. The system administrator enters a command; the system performs the requested action and responds with the result.

Refer to *Software Input/Output: Maintenance* (553-3001-511) for the complete list of maintenance programs, as well as their prompt/response sequences.

System database backup and restore

The Utilities menu of the Succession 1000 Installation program can be invoked at any time from the command line. Database archive and restore procedures are explained in the "Utilities" chapter of *Succession 1000 System: Upgrade Procedures* (553-3031-258).

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

Voice Gateway Media Card

For maintenance commands on the Voice Gateway Media Card, see "Voice Gateway Media Card maintenance" in *IP Line: Description, Installation, and Operation* (553-3001-365).

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 the Voice Gateway Media Cards.

To restore information to a Voice Gateway Media Card, use the **configFileGet** command as described in "IP Line application administration" in *IP Line: Description, Installation, and Operation* (553-3001-365).

Signaling Server CLI

A set of CLI commands is available for the Signaling Server. For CLI commands on the Signaling Server, see *IP Line: Description, Installation, and Operation* (553-3001-365).

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 backup or restore the IP telephony node files found on the Signaling Server. For more information, see *IP Peer Networking* (553-3001-213).

Element Manager

To have access to the patching feature, you must enter the administration password configured in LD 17. Patches can be downloaded from the Nortel Networks website using any web browser. From the Element Manager web pages, you can upload (see "File upload" in *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232)) and place patches into service on the Call Server, Media Gateways, and the IP telephony components (Signaling Server, Voice Gateway Media Cards).

You do not need to receive notification and software media from Nortel Networks to perform routine maintenance and upgrade tasks. All software and patches are available from the Nortel Networks Software Download website. Instructions for using the website are in the Appendix of the *Succession 1000 System: Upgrade Procedures* (553-3031-258) guide.

Call Server

Patching of the Call Server can be performed with Element Manager. See "Patching" in *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) for more information.

A data dump can be invoked from the **System Utility | Backup** menu. Similarly, there is a restore that can be invoked from the **System Utility | Restore** menu. See *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) and *IP Line: Description, Installation, and Operation* (553-3001-365) for more information.

Signaling Server

Element Manager can be used to patch IP telephony components including Signaling Servers and Voice Gateway Media Cards. Patching the Signaling Server can patch Element Manager itself. See *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) for more information.

You can also back up the Gatekeeper. See "Backing up the Gatekeeper" in *IP Peer Networking* (553-3001-213).

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 Internet Telephones as a maintenance activity when new releases of software come out. See *Succession 1000 System: Upgrade Procedures* (553-3031-258) for the procedures.

OTM

Succession 1000 systems have over 600 overlay-based maintenance commands that support their capabilities. OTM Maintenance Windows eliminates the need to remember or look up any overlay-based commands. The 37 Maintenance Overlays are grouped into eight hardware-related windows to allow you to perform all maintenance tasks. The interface provides a comprehensive view of system hardware configuration with the following benefits:

- See the equipped hardware at a glance. The hardware list works like a spreadsheet data view – you can scroll through the list, sort the list, and select items for changing.

- Select an item from the list and apply a maintenance command from the right-mouse button pop-up menu.

- Print the list or copy it to a spreadsheet.

- Select a TN or DN and print the TN/DN block.

- See Enabled/Disabled status in real time

Windows-based and web-based maintenance

The Windows- and web-based Maintenance consoles for OTM share the following tasks:

- Core CPU

- I/O Ports

- PE Shelves

- PE Cards

- B-channels

In addition, Windows-based Maintenance offers access to maintain Network Groups, Network Loops, D-channels, PE Units, and Inventory Reporting.

By contrast, Web-based Maintenance offers maintenance to Groups, Loops, and Find Telephones and Find PE units pages (which, after found, can be maintained by the tool). See "Maintenance applications" in *Optivity Telephony Manager: System Administration* (553-3001-330).

System management applications

Contents

This section contains information on the following topics:

Introduction

The following describes applications used to manage Succession 1000M, Succession 1000, and Meridian 1 systems.

History File

The History File is a file to which the system writes messages, and reduces the need for on-site TTY facilities. The contents of the file are available for problem diagnosis and can be printed at any time. Printed History File messages are prefixed by % to differentiate them from normal TTY printed output

The types of messages stored in the History File are specified on a system basis in LD 17 and can include the following:

- Maintenance messages

- TTY logins and logouts

- Regular hourly time stamps

- Service change messages, including LD commands and SCH messages

- Customer service change messages, including Attendant Administration and Automatic Set Relocation

- Traffic reports and messages (unless traffic messages are directed to a separate Traffic Log File)

- Software error messages

One history file can be specified for each system. The number of messages stored depends on the defined size of the History File and the size of the messages being stored.

The size of the History File, which resides in protected memory, can be up to 65,534 characters, or 32,767 words (one word in protected memory stores two History File characters).

The History File is a circular file: When the file is full, the system "wraps" to the beginning of the file, overwriting the oldest entry.

To further simplify accessing and reviewing messages, the History File feature supports redirecting messages to a TTY Log File or a Traffic Log File. Messages recorded in one of these files are not written to the History File. LD 17 establishes the destination of different message types.

TTY Log File

With the Multi-User Login feature enabled, the log files associated with system TTY terminals record messages including the following:

- service changes

- traffic (if not redirected to a Traffic Log File)

- CDR activity

- software bugs

Messages recorded in a TTY Log File are not written to the History File.

Traffic Log File

One Traffic Log File can be specified for each system. All system-generated traffic reports are recorded in that file rather than the History File, making these reports more accessible. The View History File (VHST) command provides access to the Traffic Log File.

View History File

LD 22 supports View History File (VHST) for selective viewing (printing) of History File and Traffic Log File contents. VHST provides a comprehensive set of commands that cause the following actions:

- display (print) a portion of the file

- search forward or backward through a file for a specific alphanumeric string

- repeat the previous search

- move up or down a specified number of lines

- go to the top or bottom of the file

See "LD 22 – VHST commands" on page 132 for a descriptive list of these commands. The HELP command displays the complete VHST command set.

In addition, regular hourly time stamps and user login/logout time stamps facilitate identifying and locating relevant messages in a large file.

Operating parameters

Create the History File in LD 17 before using VHST in LD 22.

When the History File or the Traffic Log File is full, new incoming messages overwrite the oldest stored messages. If this occurs, a FILE OVERFLOW

message and the entire existing file is printed the next time a printout is requested.

Changing the size of the History File or Traffic Log File erases all previously stored message data.

The VHST command has no impact on existing AHST (Print All History) and PHST (Print Partial History) commands.

The Traffic Log File can only be viewed (printed) using VHST. It cannot be printed with AHST or PHST.

Viewing the Traffic Log File requires that the History File be configured with a size greater than 0.

Feature interactions

System Reload and Initialization

History File and Traffic Log File information survives a system initialization. Both files are re-initialized after a system reload.

Feature packaging

History File (HIST), package 55, has no feature package dependencies. The History File package contains the Traffic Log File and VHST capabilities.

Feature implementation

LD 17 – Implement the History File feature.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action Device and Number

Note: If planning to implement a Traffic Log File, make the History File the only device with a USER of TRF. If a USER of TRF is given to a TTY Log File, the Traffic Log File may contain extraneous TTY messages.

ADAN	NEW HST	Create the History File
	CHG HST	Change the History File
	OUT HST	Remove the History File
SIZE	(0)–65534	Size of the file buffer (either History or Traffic Log).
USER	MTC SCH TRF BUG CSC	Message types to be stored in the History File. See Note below.
ADAN	<cr> ****	Go to next prompt or exit overlay.

Note: If planning to implement a Traffic Log File, make the History File the only device with a USER of TRF. If a USER of TRF is given to a TTY Log File, the Traffic Log File may contain extraneous TTY messages.

LD 17 – Implement the Traffic Log File.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action Device and Number
ADAN	NEW TRF	Create the Traffic Log File.
	CHG TRF	Change the Traffic Log File.
	OUT TRF	Remove the Traffic Log File.
SIZE	(0)–65534	Size of the file buffer (either History or Traffic Log)

LD 22 – Print or view the contents of the History File or Traffic Log File.

Prompt	Response	Description
REQ	PRT	Print

TYPE	PHST	Print all new messages stored in the History File since the file was last printed.
	AHST	Print the entire content of the History File.
	VHST	Invoke the View History File mode to view either the History or Traffic Log File.
_VHST	xxxx **	VHST command; ** to exit VHST mode

Feature operation

A response of the View History File command VHST to the TYPE prompt in LD 22 displays (prints) a segment of the History File or Traffic Log File. The printed segment includes the index, a movable marker within the file that the VHST subcommands use as their starting point.

Search strings can be up to 12 alphanumeric characters, including spaces and special characters. Double quotes are reserved for enclosing leading or trailing spaces. For example, ". "is a valid search string, composed of a period followed by three spaces.

Searches wrap when they reach the end (or beginning) of the file without finding the string. The search continues until it finds the string or returns to its starting point (the index). The VHST commands and their meanings appear in this LD 22 table.

LD 22 – VHST commands (Part 1 of 2)

Prompt	Response	Description
VHST	FIND aaaa	Starting at the index, search forward for string "aaaa".
VHST	FIND	Repeat the previous forward search.
VHST	BFIND aaaa	Starting at the index, search backward for string "aaaa".
VHST	BFIND	Repeat the previous backward search.

LD 22 – VHST commands (Part 2 of 2)

Prompt	Response	Description
VHST	UP x	Move the index backward x lines (toward the beginning of the file); display six lines beginning at the new index.
VHST	UP TOP	Move the index to the beginning of the file; display six lines beginning at the new index.
VHST	DOWN x	Move the index forward x lines (toward the end of the file); display six lines beginning at the new index.
VHST	DOWN BOT	Move the index to the end of the file; display six lines beginning at the new index.
VHST	PREV x	Move the index backward x lines, displaying all lines between the current index and location x.
VHST	PREV TOP	Move the index to the beginning of the file, displaying all lines between the current index and the beginning.
VHST	NEXT x	Move the index forward x lines, displaying all lines between the current index and location x.
VHST	NEXT TOP	Move the index to the end of the file, displaying all lines between the current index and the end.
VHST	HELP	Display the VHST command set.
VHST	% ON,% OFF	Turn on or off these display features: Brackets [ ] surrounding the index Percent sign (%) preceding each history file line (when lines are intermingled with normal TTY output) A relative percentage denoting the location of the index within the file
VHST	**	Exit VHST.

History File time stamps

In addition to the regular hourly time stamp, the History File produces a chronological sequence of user sessions by providing time-stamped messages whenever a user logs in, loads an overlay, or logs out. These messages take the following formats:

- User login message format:

  TTY #nn LOGGED IN <User Name> hh:mm dd/mm/yyyy

  Example:

  TTY #00 LOGGED IN ADAMS 13:18 05/28/93

- User program load message format:

  TTY #nn LD xxx <User Name> hh:mm dd/mm/yyyy

  Example:

  TTY #00 LD 17 ADAMS 13:19 05/28/93

Limited Access to Overlays

Limited Access to Overlays lets the administrator restrict user access to specific programs and data. 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. This feature include 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 should 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* (553-3001-311).

An administrator (who must be logged in with PWD2) can associate a user name with PWD1, PWD2, and the 100 LAPW passwords. The user name can be up to 11 alphanumeric characters. The LNAME_OPTION in LD 17, which defaults to NO, can be set to YES to indicate that login names are required. When the value is changed from NO to YES, the system assigns the default user names listed in Table 27, which the system administrator can change using LD 17.

Table 27
Default user names

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

> **CAUTION**
>
> If the LNAME_OPTION is set to YES, the system
> accepts non-unique passwords (because it uses the
> login name as the unique user identifier). If the
> LNAME_OPTION is then set to NO, the system
> creates a new, random password for each password.
> This is to ensure that the passwords, which are now
> the unique identifier for each user, are indeed unique.
> When the system reassigns passwords, it issues a
> message indicating the new PWD2 password. Make
> note of this password, as it must be used to access
> LD 17 to change it and any other password.

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

- leftwise unique (if login name option is NO)

- different from existing passwords (if login name option is NO)

For example, acceptable passwords may include

- JSMITH

- 0001

- 2GUEST

- TECHNICIAN

Using LD 17, a system administrator logged in with PWD2 can define user
access to overlays. If a user tries to access a restricted overlay, a message
appears and access is denied.

The administrator can also restrict access to certain commands within a given
overlay. For example, the administrator can specify **print only** access for a

password. Users logged in with that password are restricted to print commands within an overlay. Any other user requests generate the following system message:

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

The system monitors login attempts for attempted security breaches. Failed attempts with invalid passwords are counted and the tally is compared with a predefined threshold. If the threshold is met or passed, the entry point (TTY or terminal) is locked out for a predetermined time (set through a service change and password protected). The system ignores attempted access from that entry point until the lockout timer expires.

Lockout conditions are reported to all maintenance terminals when they occur, with a special report to the next system administrator who logs in.

The system can keep an Audit Trail to record login information. The Audit Trail printout includes 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

where:

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 28
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

Only system administrators logged in using PWD1 or PWD2 can access the Audit Trail from LD 22.

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 LAPW feature should only be enabled on a system that has a completed configuration record in LD 17 and that is already up and running.

If LNAME_OPTION in LD 17 is set to YES, the system assigns unique login names for all passwords, including PWD1 and PWD2. See Table 27 on page 135.

With LNAME_OPTION left at NO (the system default), 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 Caution on page 136.

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 this feature.

Feature packaging

This feature requires Limited Access to Overlays (LAPW) package 164, which must be enabled for this feature to operate.

Feature implementation

Implementing the LAPW feature requires the Configuration Record (CFN), LD 17 to be changed. Respond to the following prompts in LD 17.

LD 17 – Define LAPW options and passwords. (Part 1 of 3)

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	(NO) YES	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.

LD 17 – Define LAPW options and passwords. (Part 2 of 3)

Prompt	Response	Description
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.
- CUST	(XALL) 0–99 0-31 ALL	(No customers), customer number, or all customers Customer number for Large Systems. Customer number for Small Systems and Succession 1000 systems. 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).

LD 17 – Define LAPW options and passwords. (Part 3 of 3)

Prompt	Response	Description
	(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.

LD 17 – Change user's LAPW password (user must log in using current LAPW).

Prompt	Response	Description
REQ	CHG	Change
PWD2	<cr>	Level 2 master password
- LPWD	aaaa	Login Password for LAPW user
- NLPW	xx...x	New login password for LAPW user

LD 22 – Print options available for LAPW passwords (administrator). (Part 1 of 2)

Prompt	Response	Description
REQ	PRT	Print
TYPE	PWD	Password

LD 22 – Print options available for LAPW passwords (administrator). (Part 2 of 2)

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	aaaa…	Password options allowed
Note: LAPW password options are output to the active TTY only.		

LD 22 – Print options for LAPW password (user).

Prompt	Response	Description
REQ	PRT	Print
TYPE	PWD	Password
PWD2	<cr>	Administrator's 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 numbers accessible
Host	No	Host mode
OPT	aaaa…	Password options allowed
PWxx	aaaaaa...	LAPW password number and password
Note: Options available to the logged on password are printed.		

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>

>

Note: Only one space is accepted between LOGI and the login name. If more than one space is entered, the system ignores the login name.

For information on setting and changing LAPW passwords after successful login, see "Feature implementation" on page 139.

Meridian Mail Voice Mailbox Administration

The Meridian Mail Voice Mailbox Administration (VMBA) feature enables the system administrator to use system administration overlays to administer and maintain the Meridian Mail Voice Mailbox application. This feature streamlines the process of implementing and maintaining Voice Mailboxes (VMBs).

VMBA provides the following capabilities:

• accessing the Voice Mailbox Application through LDs 10 and 11 rather than through a separate terminal

• viewing application and mailbox statistics to help ensure the integrity of the application

• synchronizing 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. The system administrator can run the audit manually or request that the system run it periodically.

— For sites that want to implement VMBA and already have VMBs configured on Meridian Mail, the VMBA upload function lets the system administrator create or update the system VMB database from the existing Meridian Mail VMB database. Upload can significantly reduce the time required to implement VMBA.

Access to Meridian Mail VMB administration functions is still available with 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* (553-3001-306).

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

In addition to the data transmission parameters supported for an MSDL SDI port, a set of functions can be specified for the port. The functions include 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, available on other cards that support SDI, are also 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

Autobauding is the ability of 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

then sends a message showing the baud rate to the SDI port. Autobauding helps eliminate the problem of baud rate mismatches causing a port lockout.

Line Mode Editing

Line Mode Editing (LME) permits the user to 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.

XON/XOFF handling

XOFF suspends data output from an MSDL SDI data port; XON resumes data output. The MSDL card stores up to 500 characters in its buffer. When the capacity is exceeded, newer data overwrites existing 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. The MSDL SDI can be configured to screen invalid characters before transmitting them 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

This function enables the SDI application to determine if the modem for the SDI port is currently connected and operational. If it is not, no output is sent to, nor input received from, the modem. This eliminates the problem caused by smart modems echoing characters received from the system.

DTR/CTS detection

When the MSDL SDI is configured as DCE, it monitors the DTR signal. When it is configured as 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 a technician disables 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 29.

Table 29
Available port functions

	Autobaud	Modem Support	XON/XOFF Handling	Line Mode Editing	Character Screening
Maintenance TTY (Note 1)	Yes	Yes	Yes	Yes	Yes
Application TTY (Note 2)	Yes	Yes	Yes	Yes	Yes
Application Link (Note 3)	No	Yes	No	No	No
System Monitor XSM	No	No	No	No	No
PRT	No	Yes	Yes	No	No
Note 1: User types of BUG, CSC, MTC, SCH, FIL					
Note 2: User types of TRF, CTY, BGD					
Note 3: User types of ACD, APL, HSL, PMS					

None of the functions applies to a system power port (an SDI defined with XSM = YES and USER = MTC).

Figure 5 on page 150 illustrates the software components that comprise the MSDL SDI, showing the different functional units.

Operating parameters

An SDI port on the MSDL is set up with full duplex communication. The configurable data transmission parameters are listed below, with defaults in parentheses. To change a default setting, use LD 17.

• Cable connection: (RS–232), RS–422

Figure 5
MSDL SDI software components
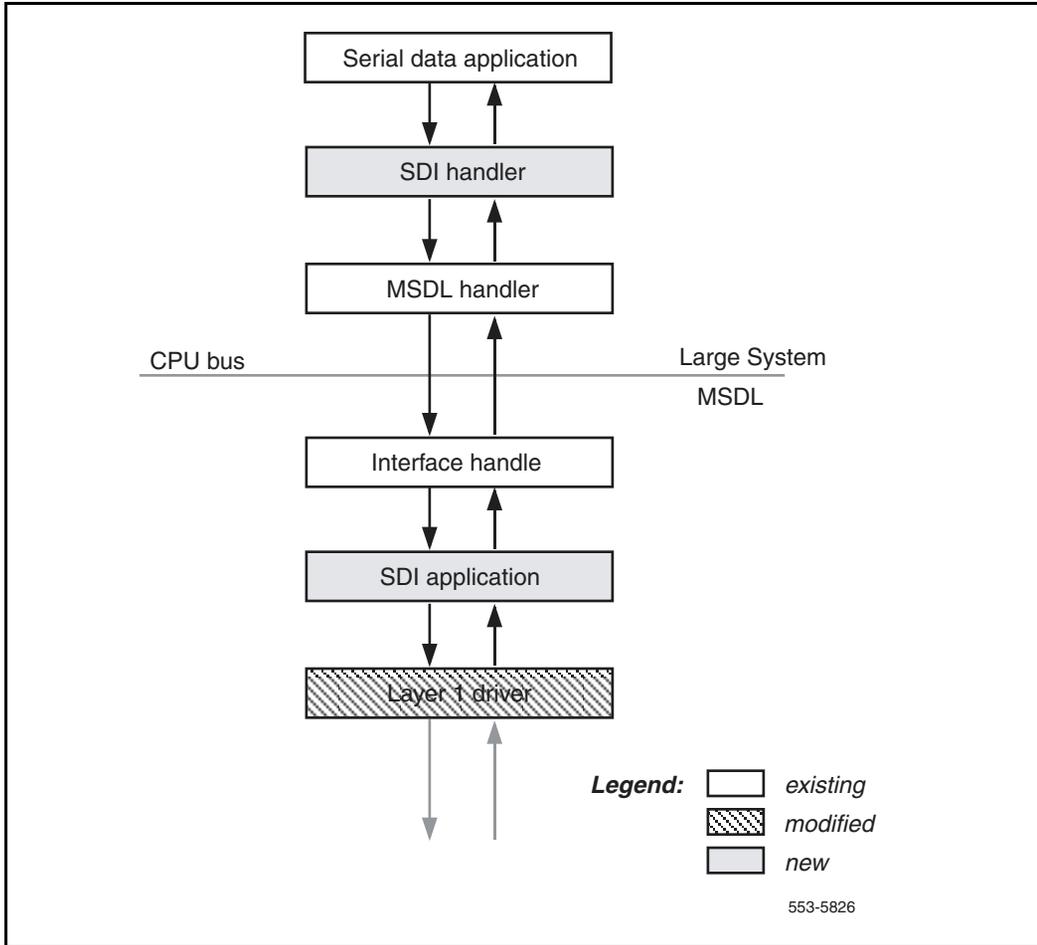
- Baud rate: 300, 600, (1200), 2400, 4800, 9600, 19200, or 38400 bps

- 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.

   Note: If the number of data bits specified is 8, the system typically transmits the high order bit as 1. A terminal that is not equipped to handle this data will not display characters properly. In Line Mode Editing (LME), the MSDL provides proper 8-bit output.

To abort a self-test running on an MSDL port, enter "END".

   Note: A string of four asterisks (****) does not abort the self-test.

Changing the configuration for an MSDL port, such as changing baud rate or activating autobaud support, does not take effect until the port is disabled and re-enabled manually through a maintenance overlay, or until it is re-enabled through a manual initialization.

Unlike other SDIs that send output regardless of the state of the RS-232 signals, the MSDL SDI only sends output if the DTR (for DCE) or CTS (for DTE) signal is high.

Setting breakpoints from an MSDL SDI is not supported.

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

The MSDL SDI port can be connected to an auxiliary port. If the auxiliary port does not use the MSDL SDI functions (such as autobauding and line mode editing), then its operation is unaffected. If the AUX does operate with some or all of the new MSDL SDI functions, modification of other applications may be necessary.

If an MSDL SDI card is used with a modem that has been configured for the Property Management System Interface (PMSI) link, the MSDL SDI driver cannot transmit or receive a message without the modem connection. If modem power is off or the modem cable is loose, the system periodically polls PMS. Since there is no modem connection, the polling message is not delivered, and the system assumes that the link is not responding.

Feature packaging

This feature 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 are the implementation limitations:

- 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 set 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.

LD 17 – Configure MSDL SDI. (Part 1 of 3)

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
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

LD 17 – Configure MSDL SDI. (Part 2 of 3)

Prompt	Response	Description
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

LD 17 – Configure MSDL SDI. (Part 3 of 3)

Prompt	Response	Description
	MTC	Maintenance
	NOO	No Overlay allowed
	PMS	Property Management System interface
	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

LD 17 – Prompts and responses for Sample 1. (Part 1 of 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	MDSL	Multi-purpose Serial Data Link card type

LD 17 – Prompts and responses for Sample 1. (Part 2 of 2)

Prompt	Response	Description
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
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 set to the same parameters: 9600 baud, no parity, 7 data bits, 1 stop bit.

Note 2: Because the SDI port is DCE, the terminal will be 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

LD 17 – Prompts and responses for Sample 2. (Part 1 of 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
BITL	7	Data bit length

LD 17 – Prompts and responses for Sample 2. (Part 2 of 2)

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

LD 17 – Prompts and responses for Sample 3. (Part 1 of 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	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

LD 17 – Prompts and responses for Sample 3. (Part 2 of 2)

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
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

LD 17 – Prompts and responses for Sample 4. (Part 1 of 2)

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

LD 17 – Prompts and responses for Sample 4. (Part 2 of 2)

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

LD 17 – Prompts and responses for Sample 5. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change

LD 17 – Prompts and responses for Sample 5. (Part 2 of 2)

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.

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.

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 1 minute. After a 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 set up for an RS-232 interface, no printing occurs.

Figure 6
Line Mode Editing display

```
ADAN  TTY 0
 CTYP SDI2
 DNUM 0
 USER MTC TRF SCH BUG CSC BGD
 CUST 01
 XSM NO
ADAN TTY 1
 CTYP SDI2
 DNUM 1
 USER TRF
 XSM NO
ADAN  TTY 6
 CTYP SDI2
 DNUM 6
 USER ACD
 CUST 01
 SSUP NO
 APRT YES
```

Output area

```
==> END
```

553-5908

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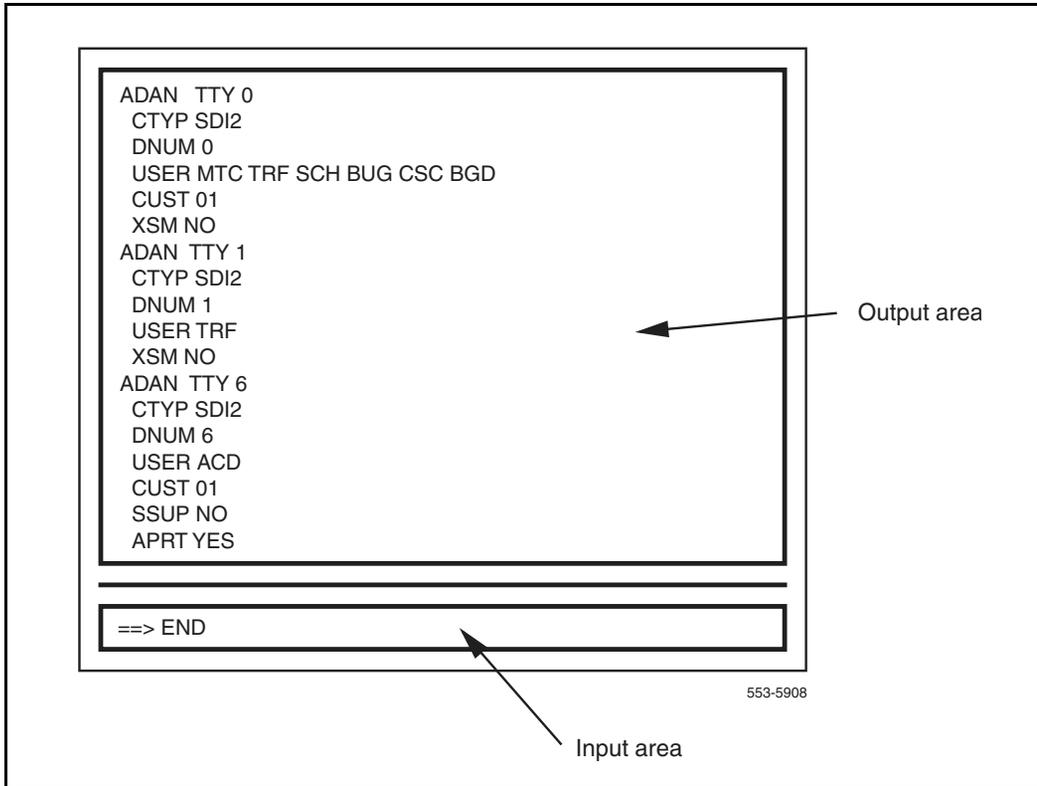
If the MSDL is enabled (with base code running), SDI ports will output sysload messages if the SDI application has also been enabled; otherwise, no messages print.

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.

Multi-User Login also introduces several new user commands. With these commands, the user has the ability to:

- communicate with other users

- determine who is logged into the system

- halt and resume background and midnight routines

- initiate and terminate terminal monitoring

- change printer output assignment

See "User commands" on page 170 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 new 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" on page 168 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. It 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. For more information about PTYs, see the *Succession 1000 System: Installation and Configuration* (553-3031-210).

OTM

With OTM it is possible to have multiple administrators logged in and schedule changes at the same time to one or more Succession 1000M, Succession 1000, and Meridian 1 systems. On a single system users could be accessing Maintenance Windows, CDR records could be collected by DBA, and Station Administration changes could be occurring simultaneously.

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, 44, and 80 can run at a time, but they each can run with other overlays.

- Multiple copies of LD 10, 11, 20, 21, and 22 can run at a time.

Valid overlay combinations are shown in Table 30, on page 168.

Feature interactions

Nortel Networks 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, system administrators 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" on page 134 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 30
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)
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.

LD 17 – Activate Multi-User Login. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change

LD 17 – Activate Multi-User Login. (Part 2 of 2)

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.

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	Change LAPW password nn
	<cr>	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

LD 22 – Print TTYLOG and MULTI_USER values. (Part 1 of 2)

Prompt	Response	Description
REQ	PRT	Print
TYPE	ADAN TTY n	Print TTYLOG value if USER = MTC, SCH, TRF, BUG, or FIL

LD 22 – Print TTYLOG and MULTI_USER values. (Part 2 of 2)

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 31 on page 171 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

Set-Based Administration

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

Table 31
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).
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.

- Administration Access allows a system administrator to make changes to any supported telephones within the same customer location. The system administrator can perform any of the following tasks through an administration/maintenance set (M2008, M2016, M2216, M2616 with display):

    — Change the data associated with specific set-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 set.

        – Determine Directory Number-Terminal Number correspondence.

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

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

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

    — Change system data and time.

    — Change toll restriction for that set.

User Installation allows a user to add or change the user's own SPND when logging in through the user's own set.

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 set.

As well as displaying useful information on the set's display, sound cues are employed for the benefit of users logged into Set-Based Administration (SBA) on sets without displays. Four seconds of overflow tone indicates the user made an error, while four seconds of special dialtone 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 set's PROGRAM key.

For a Small System or Succession 1000 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 the above 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 set using this feature.

The CPND name change enhancement to Set-Based Administration is not supported using non-display sets, 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 set 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 sets 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 will prevent 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 set or Installer set 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 set 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 Set becomes an Administration set 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.

Data Dump

Login is not permitted while a data dump is in progress. The result will be 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 will be 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 will be 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 will also cause the ODAS time stamps to be updated.

Remote Call Forward

A set may be remote call forwarded while someone is actively logged into 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 will interact 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 and Succession 1000)

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 set

- 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.

LD 17 – Define Set-Based Administration passwords. (Part 1 of 2)

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
...		
- 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
- OPT		Specify permissions and restrictions associated with Set-Based Administration password PWNN. At least one permission must be given. The default is no permissions.

LD 17 – Define Set-Based Administration passwords. (Part 2 of 2)

	(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.

LD 57 – Define Set-Based Administration FFCs. (Part 1 of 2)

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
...		

LD 57 – Define Set-Based Administration FFCs. (Part 2 of 2)

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 have been introduced by this feature. For a complete description of the Set-Based Administration feature, refer to *Set-Based Administration* (553-3001-303).

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		Terminal number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
...		
CLS	MTA	Maintenance allowed Class of Service

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.

LD 17 – Increase the Maximum Number of Logins. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change
TYPE	PARM	Parameters data
...		

Only accepted if ADMINSET package is equipped.

LD 17 – Increase the Maximum Number of Logins. (Part 2 of 2)

SBA_ADM_INS	0-(1)-2	Maximum Administrator and/or Installer logins allowed at one time (see Note) For Small Systems
	0-(2)-64	For Large Systems
SBA_USER	0-(10)-20	Maximum User logins allowed at one time (see Note) For Small Systems
	0-(100)-500	For Large Systems
Only accepted if ADMINSET package is equipped.		

LD 17 – Increase buffers.

Prompt	Response	Description
REQ	CHG	Change
TYPE	PARM	Parameters data
...		
500B	75	Number of output buffers

LD 15 – Enable use of Station Control Passwords. (Part 1 of 2)

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	FFC	Flexible Feature Code
...		
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>.		

LD 15 – Enable use of Station Control Passwords. (Part 2 of 2)

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>.

LD 10, LD 11 – Assign User Access Allowed Class of Service. (Part 1 of 2)

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	xxxx	Type of set to be changed.
TN		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
...		

LD 10, LD 11 – Assign User Access Allowed Class of Service. (Part 2 of 2)

SCPW	xxxx	Station Control password for this set
CLS	(ULAD) ULAA	(Deny) Allow User level access to Set-Based Administration.

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* (553-3001-211) 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 7
An STA-monitored system with STA administration and regular terminals
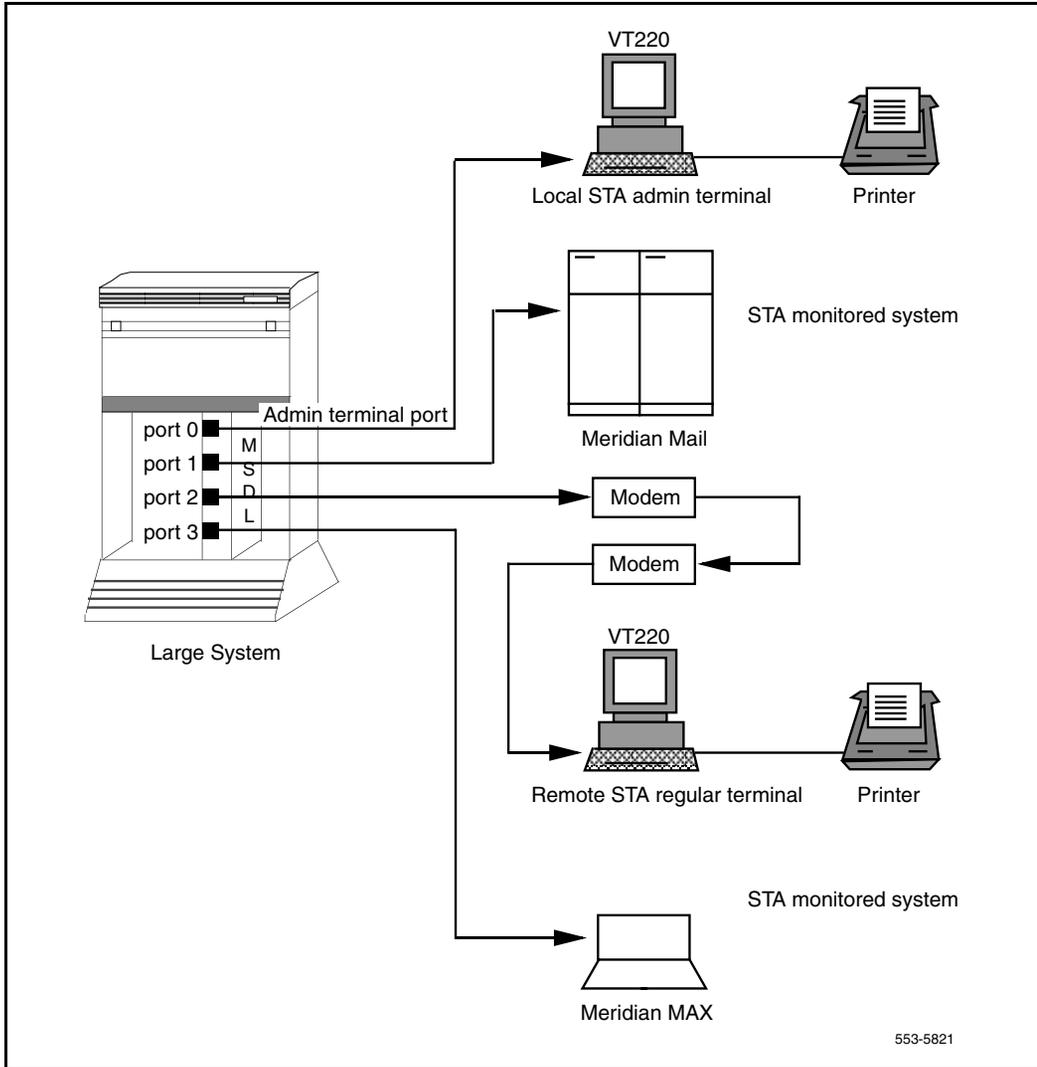
Functions

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" on page 147.

- 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 32.

Table 32
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 33 for possible port assignments.

Table 33
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		
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, 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 8 on page 192. 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.

On page 208 is an STA Planning Form to assist in preparing for an STA implementation.

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:

1   Verify that MSDL package 222, MSDL SDI package 227, and STA package 228 software is 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" on page 145 for assistance.

Figure 8
STA cable and connection information

MSDL

STA

NTND27AB

(RS232/DCE)

DB25

Regular 25-pin Cable*

VT220

Port J9

NT7D46AA

Regular 25-pin Cable*

(RS232/DTE)

DB25

DB9

Null Modem
Adaptor (25–25)
[303-3, M-F][1]

Meridian Link
Meridian MAX
Meridian CCR
Meridian 911

9–25 Pin Converter
[358-4,F-F][1]

DB9
Console Port on
MVME712A/AM Card

NT6D4405

Regular 25-pin Cable*

(RS232/DTE)

DB25

DB25

Meridian Mail

Maintenance Console Port (DB9)
on ESBC Card

Meridian 1 I/O Panel

Aux System Back Panel

Male Side ⟶ 〈 ⟵ Female Side

553-5855

*This cable can be obtained off the shelf or from NT. NT has male-male: NT1R03DB (2 feet), NT1R03DC
(4 feet), NT1R03DF (10 feet), NT1R03DP (25 feet), NT1R03DV (45 feet); and male-female: NT1R03EB
(2 feet), NT1R03EC (4 feet), NT1R03EF (10 feet), NT1R03EP (25 feet), NT1R03EV (45 feet). Shown in this
figure are male-male cables.

3   Prepare a VT220 terminal for this port. Table 34 shows the recommended general setup for the STA terminal. The items that appear in bold are of particular importance. "Terminal setup for STA" on page 205 shows the setup for a VT420 terminal.

Table 34
Recommended setup for the STA terminal (Part 1 of 2)

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**

Table 34
Recommended setup for the STA terminal (Part 2 of 2)

Communications Parameters:	
Parameter	**Default STA Terminal Setup**
Transmit Baud	2400–19200
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.

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)
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" on page 199 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 STA Planning Form on page 208. Also, arrange the port configuration using the information in Table 35, "Recommended port configurations for STA-monitored systems," on page 203.

- 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" on page 200.

- 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.

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 if the MSDL does not have the STA application loaded or if the STA application on the MSDL is a different version from the one resident on the system disk. The user can specify the Firmware Download (FDL) option.

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.

- Detects an escape sequence from the user, sending 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 only be established 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 RS232 (or RS422) 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 the user 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 the user has changed the STA application-level configuration, it will not be downloaded.

If the STA application is up and running and MSDL base code or the STA application must be downloaded, STA is temporarily suspended. After an INIT, the STA application is restored.

If the application is not up and running, 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:

1   Use LD 48 to disable the STA application.

2   Remove the STA application using LD 17.

To remove an MSDL port from STA:

1   Use LD 48 to disable the STA application.

2   Use LD 17 to remove the port.

Feature operation

Maintenance commands

There are three classes of maintenance commands for the STA application: MSDL card, STA application, and STA port.

MSDL card commands

Commands in LDs 37, 42, 48, and 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

New 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 9 on page 201 shows the structure of the STA menus.

To select an STA operation from the STA Main Menu (see "STA Main
Menu" on page 202), the user either presses the designated function key or
moves the highlight bar to an operation and presses <CR>.

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 the user 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.

Figure 9
STA menu structure

Figure 10
STA Main Menu

```
                    STA Main Menu

          F6  View Port Configuration

          F7  Change Port Configuration

          F8  Port Maintenance

          F9  Access Options

          F10 Connect to  Large System

          F11 Connect to Meridian Mail


        Meridian 1 Single Terminal Access Port Status

 MSDL Port:    0              1          2          3
 Port Name:    Admin Terminal MODEM                 Meridian Mail
 Port Status:  enabled        enabled    non-STA    enabled
```

553-5822
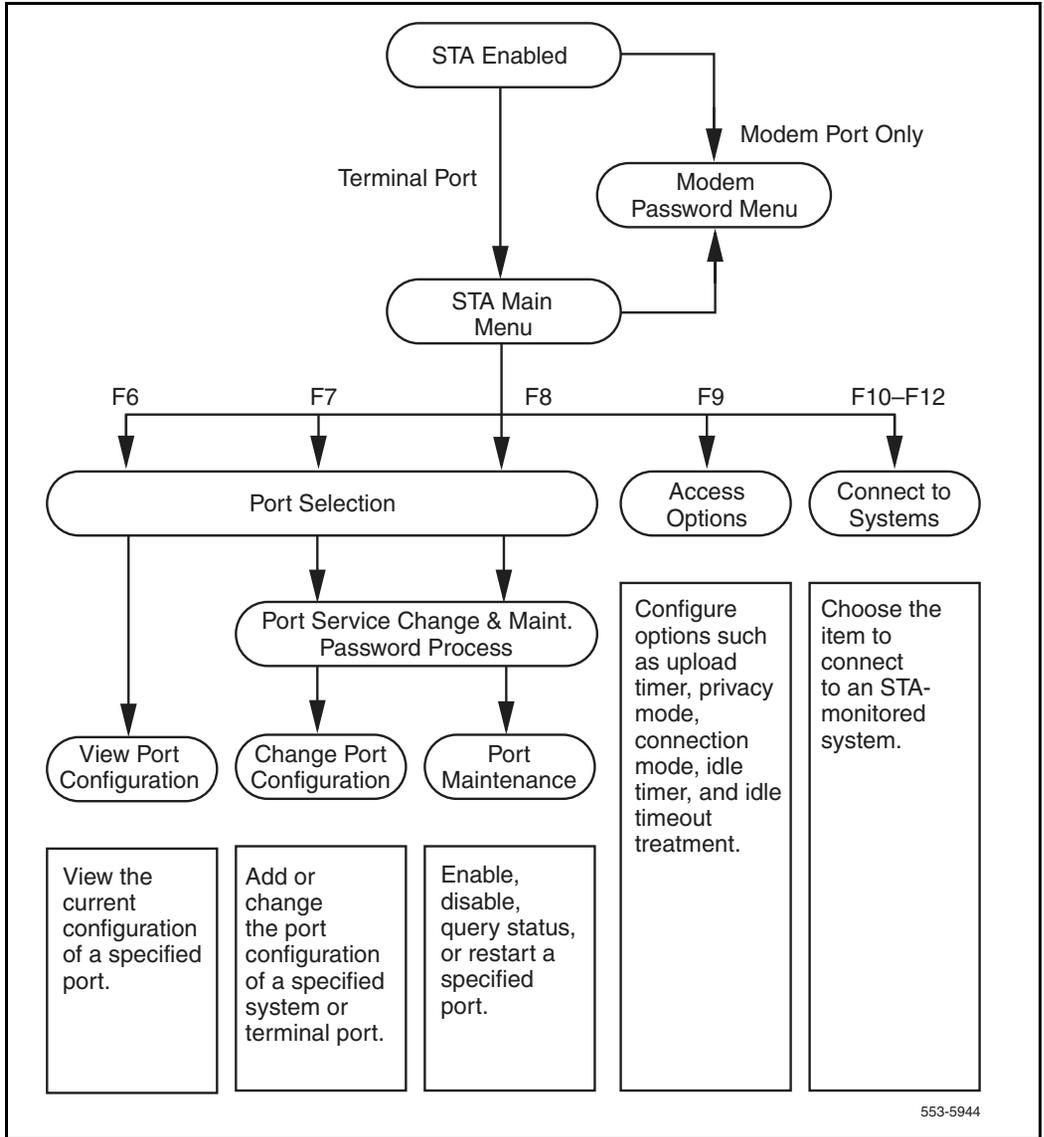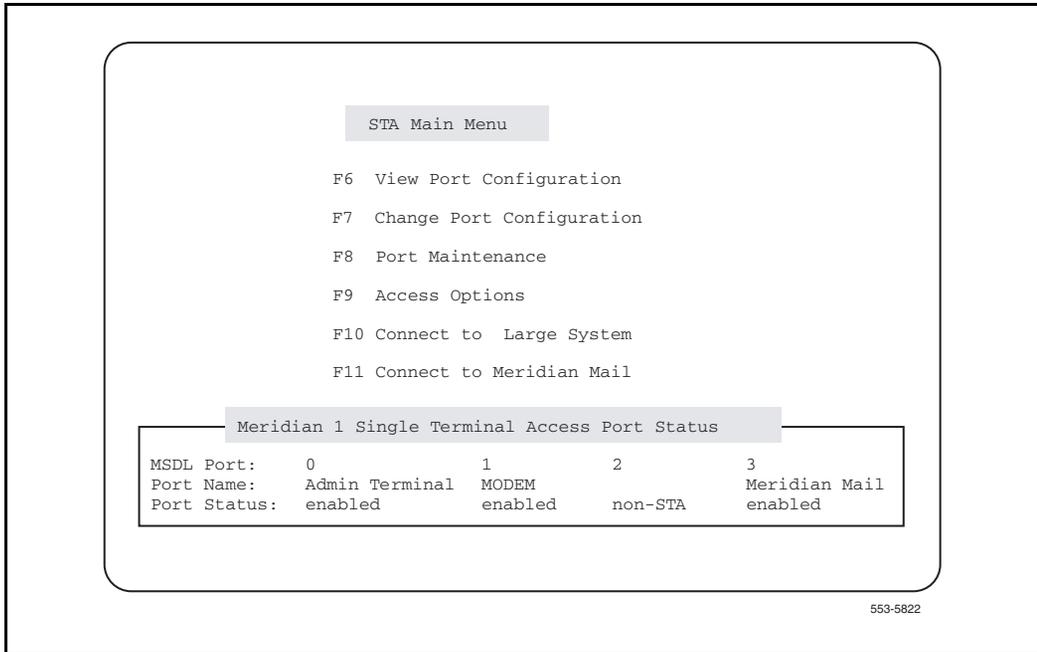
> *Note:* If LAPW is equipped, the user name can be up to 11 characters
> and the password up to 16 characters in length. The password is
> configured under the NPW1, NPW2, or PW00–99 prompts in LD 17. If
> the LNAME_OPTION is off, no login name is required.

After validating the user's entries, the operation displays the port information.
To change an entry, the user moves the highlight bar to the entry, then uses
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.The user can view, but cannot change, the STA
administration terminal configuration. It must be changed through LD 17 and
downloaded when STA is enabled.

Table 35 lists the recommended port configurations for connecting to STA-monitored systems.

Table 35
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*
	* EM100 emulation mode is required for a VT220 to operate on a VT100-supported STA-monitored system.		

F8 Port Maintenance

This operation prompts the user to select a port and enter the system password (unless the user has already done so during Change Port Configuration). After validating the user's 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, on which the user 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 36.

Table 36
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 bottom 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 the user enters more than ten invalid login name/password combinations, the menu locks and accepts no more input. The user 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 ™ 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 permits the user to map all keys on an extended keyboard to user-defined control sequences. To ensure proper operation, a user must set up 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		

Communications 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 11 on page 209 illustrates an STA planning form.

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

Figure 11
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

provides a descriptive explanation of the event. It supports Look Up Last Error and Look Up Any System Message. See "Feature operation" on page 210 for information about how to use this utility.

Operating parameters

The help text file contains about 10,000 entries and requires about 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, the user enters

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, the user enters

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 it contains special characters), the system issues the following message:

ABCDxxxx is not a valid error code.

Administration

Contents

This section contains information on the following topics:

Introduction

The following describes the loads used to administer Succession 1000M, Succession 1000, and Meridian 1 systems.

LD 117

LD 117 allows the system administrator to do the following:

- configure the Alarm Management feature

- identify all system alarms

- configure IP network interface addresses

- perform all IP network related maintenance and diagnostic functions

LD 117 uses a command line input interface (input parser) which has the following general structure (where "=>" is the command prompt):

=> COMMAND OBJECT [(FIELD1 value) (FIELD 2 value)...
(FIELDx value)]

LD 117 offers the administrator the following configuration features:

- **Context Sensitive Help** – Help is offered when "?" is entered. The Help context is determined by the position of the "?" entry in the command line. If "?" is entered in the COMMAND position, Help text will appear which presents all applicable command options. If "?" is entered in the OBJECT position, HELP text will appear which presents all applicable OBJECT options.

- **Abbreviated Inputs** – The input parser recognizes abbreviated commands, objects and object fields. For example, "N" can be entered for "NEW" or "SEV" can be entered for "Severity".

- **Optional Fields** – Object fields with default values can be bypassed by the user on the command line. For example, to configure an object which consists of fields with default values, enter the command, enter the object name, press <return>, and the object will be configured with default values. All object fields do not have to be specified.

- **Selective Change** – Instead of searching for a prompt within a lengthy prompt-response sequence, "Selective Change" empowers the administrator to directly access the object field to be changed.

- **Service Change Error Message Consistency** – The parser simplifies usage of service change error messages. LD 117 displays only SCH0099 and SCH0105.

Alarm Management

The Alarm Management feature provides a single output point for all alarms, while also improving the logging facility and making alarms more meaningful. Alarm Management provides the following features:

- Alarm Notification
- Alarm Cleanup

With the exception of the Alarm Notification and Cleanup subfeatures, this feature is optional.

Alarm Notification

The Major alarm LED on the attendant consoles is lit when a power failure occurs; however, the lamp is not lit from a central location based upon alarm

severity. The severity of these alarms are determined by the Event Server or by the Fault Management Filter and Exception table.

The system now has three alarm severities:

- critical

- major

- minor

The Minor alarm lamp on the attendant consoles lights when critical alarms occur.

Alarm Clean-up

The Alarm clean-up subfeature improves the message content and/or consistency of the system alarms. These alarms are centralized to ensure they are captured under the new Event Handling mechanism.

Alarm Management capability

With the Alarm Management feature, all processor-based system events are processed and logged into a disk-based System Event List (SEL).

Events which are generated as a result of administration activities, such as SCH or ESN error messages, *are not* logged into the SEL.

Events which are generated as a result of maintenance or system activities, like BUG and ERR error messages, *are* logged into the SEL.

Unlike the System History File, the System Event List survives Sysload, Initialization and power failures.

Event Handling

Previously, the system History File content was lost after a SYSLOAD. With this feature, a new disk-based log file, called the "System Event Log" will survive any SYSLOAD, system initialization, or power failure. Users can access the System Event Log by using LD 117.

The Event Collector

The Event Collector captures and maintains a list of all processor-based system events. The Event Collector also routes critical events to FIL TTY ports and lights the attendant console minor alarm lamp as appropriate. The System Event List (SEL) can be printed or browsed.

The Event Server

The Event Server consists of two components:

- Event Default Table (EDT): This table associates events with a default severity. By using the CHG EDT command in LD 117, the EDT can be overridden so that all events default to a severity of either INFO or MINOR. The EDT can be viewed in LD 117.

Table 37
Sample Event Default Table (EDT)

Error Code	Severity
ERR220	Critical
IOD6	Critical
BUG4001	MInor

Note: Error codes which do not appear in the EDT will be assigned a default severity of MINOR.

- Event Preference Table (EPT): This table contains site-specific preferences for event severities as well as criteria for severity escalation and alarm suppression. The administrator can configure the EPT to:

— override the default event severity assigned by the default table

— escalate event severity of frequently occurring minor or major alarms

Table 38
Sample Event Preference table

Error Code	Severity	Escalate Threshold (events/60 sec.) (see Note 2)
ERR??? (see Note 1)	Critical	5
INI???	Default	7
BUG1??	Minor	0
HWI363	Major	3
Note 1: The"?" is a wildcard.		
Note 2: The window timer length defaults to 60 seconds. However, this value can be changed by the Administrator. Read "Global Window Timer Length" on page 218 for more information.		

Wildcards

The special wildcard character "?" can be entered for the numeric segment of an error code entry in the EPT to represent a range of events. All events in the range indicated by the wildcard entry can then be assigned a particular severity or escalation threshold.

For example, if "ERR????" is entered and assigned a MAJOR severity in the EPT, all events from ERR0000 to ERR9999 are assigned MAJOR severity. If "BUG3?" is entered and assigned an escalation threshold of 5, the severity of all events from BUG0030 to BUG0039 will be escalated to the next higher severity if their occurrence rate exceeds 5 per time window.

Escalation and suppression thresholds

The escalation threshold specifies a number of events per window timer length that when exceeded, will cause the event severity to be escalated up one level. The window timer length is set to 1 minute by default. Escalation occurs only for minor or major alarms. Escalation threshold values must be less than the universal suppression threshold value.

A suppression threshold suppresses events that flood the system and applies to all events. It is set to 15 events per minute by default.

Global Window Timer Length

Both the escalation and suppression thresholds are measured within a global window timer length. The window timer length is set to 1 minute by default. However, the window timer length can be changed by using the CHG TIMER command in LD 117.

Format of TTY Event Output

TTY Event Output can be formatted or unformatted. Formatted output is also called Fancy Format. Output format is configurable in LD 117 using the CHG FMT _OUTPUT command.

Fancy Format Output

Formatted output appears in the following template:

<severity> <report id> <date> <time> <prim_seq_no> <cp_id> <cp_ad>
DESCTXT: <descriptive text>
OPRDATA: <operator data>
EXPDATA: <expert data>

Table 39
Formatted output (Part 1 of 2)

Field	Description
<severity>	"***" (critical); "**" (major); "*" (minor); " " (blank for info)
<report id>	The report id consists of an event category (for example, BUG, ERR) and an event number (for example,1200, 230.). It is padded with blanks at the end to ensure it is 9 characters long (4 characters max. for category and 5 digits max. for number). Examples of report ids are: ERR230, ACD3560, and BUG30.
<date>	DD/MM/YY
<time>	HH:MM:SS
<prim_seq_no>	Primary sequence number of the event (length of 5 digits)

Table 39
Formatted output (Part 2 of 2)

Field	Description
<cp_id>	The Component ID is a 15 character string which indicates the id of the subsystem generating the alarm.
<cp_ad>	The Component address is a 15 character string which indicates the address of the subsystem generating the event.
<descriptive text>	This is an optional string which describes an event.
<operator data>	This is an optional field which holds a 160 character string containing extra text or data to assist the operator in clearing a fault. This field contains any data output with a filtered alarm (e.g. loop number, TN, etc.).
<expert data>	This is an optional variable length character string which contains extra text or data for a system expert or designer.

The following are samples of fancy format output:

```
*** BUG015 15/12/95  12:05:45  00345
EXPDATA: 04BEF0FC 05500FBA  05500EE2  05500EC6 05500EAA
BUG015 + 05500E72 + 05500E56 + 0550D96 + 055053A + 04D84E02
+ 04D83CFC
BUG015 + 04D835CA 04D81BAE 04D7EABE 04F7EABE 04F7EDF2
04F7EFC 04F7E1B0
```

```
*    ERR00220 15/12/92 12:05:27 00346
OPRDATA: 51
```

```
     VAS0010 15/12/92 12:06:11 00347 VMBA    VAS 5
```

Unformatted Output

Unformatted data consists of only the report ID and perhaps additional text. The following is a sample of unformatted output:

```
BUG015
BUG015 + 04BEF0FC 05500FBA 05500EE2 05500EAA 0550E8E
BUG015 + 05500E72 05500E56 05500D96 0550053A 04D84E02
```

```
BUG015 + 04D835CA 04D81BAE 04D7EABE 04F7EDF2 04F7E2FC
04&E1B0
BUG015 + 04F7E148
```

ERR00220 51
VAS0010

Ethernet

LD 117 can be used to configure and manage an IP network interface. The
system is hardware-equipped for this with an Ethernet controller on the I/O
Processor (IOP) card. Each IOP card is equipped with a Local Area Network
Controller for Ethernet (LANCE) which is preconfigured with a unique
Ethernet address.

An Ethernet address is a unique 48-bit long physical address assigned to the
Ethernet controller on the IOP. On a single CPU system, there is only one IOP
which contains one Ethernet interface and an IP address which must be
configured. Single CPU systems use only a Primary IP address.

On a redundant or dual CPU system, two IP addresses must be specified:
Primary and Secondary. A dual CPU system operating normally uses the
Primary IP address. A dual CPU system operating in split mode (the mode
used only when upgrading software or hardware) uses the Secondary IP
address.

Remote Access

Remote access to the system is possible with Point-to-Point Protocol (PPP).
LD 117 can be used to configure IP addresses for Point-to-Point Protocol.

LD 117 – Configure IP addresses for Point-to-Point Protocol. (Part 1 of 2)

Prompt	Response	Description
****	Abort	Abort overlay.
BROWSE	Browse	Browse an existing System Event List.
CHG	Change	Change/modify object configuration.

LD 117 – Configure IP addresses for Point-to-Point Protocol. (Part 2 of 2)

Prompt	Response	Description
DIS	Disable	Disable Point-to-Point Protocol.
ENL	Enable	Enable Point-to-Point Protocol.
NEW	New	Add and configure new object.
OUT	Out	Delete existing object.
PRT	Print	Print configuration of existing object.
RST	Reset	Reset Object.
SET	Set	Set ELNK subnet mask to configured value.
STAT	Status	Display object statistics.
UPDATE	Update	Update INET database.

LD 117 – Command descriptions. (Part 1 of 2)

Object	Description
DBS	Database
EDT	Event Default Table: Table of default event entries and associated severities
ELNK	Ethernet interface
ELNK ACTIVE	Active Ethernet Link: Change the Primary IP address and host name
ELNK INACTIVE	Inactive Ethernet Link: Change the Secondary IP address and host name
EPT	Event Preference Table: Table of customer's event entries with associated severities

LD 117 – Command descriptions. (Part 2 of 2)

Object	Description
FMT_OUTPUT	Formatted Output: Determine if system events uses formatted (also called fancy) or unformatted output. See "Format of TTY Event Output" on page 218 for more information.
HOST	Host name
MASK	Subnet mask
OPEN_ALARM	Open Simple Network Management Protocol (SNMP) traps setting
PPP	Point-to-Point Protocol interface
PPP LOCAL	Local Point-to-Point Protocol interface address
PPP REMOTE	Remote Point-to-Point Protocol interface address
PTM	Point-to-Point Protocol idle Timer
ROUTE	Configure new routing entry
SELSIZE	System Event List Size: Number of events in System Event Log
SEL	System Event List
SUPPRESS	Suppress count: Number of times the same event is processed before it is suppressed
TIMER	Global window timer length. See "Global Window Timer Length" on page 218 for more information.

LD 117 – Administration commands

The commands listed below use the following general structure (where "=>" is the command prompt):

=> COMMAND OBJECT [(FIELD1 value) (FIELD 2 value)... (FIELDx value)]

In Table 40, COMMANDS and OBJECTS are in bold typeface and fields are in regular typeface. Fields enclosed in brackets ( ) are default values.

Table 40
Commands and Objects (Part 1 of 8)

=> **Command**	**Description**
BROWSE SEL UP n	Browse up n # of lines in System Event List (SEL).
BROWSE SEL DOWN n	Browse down n # of lines in SEL.
BROWSE SEL TOP	Browse to top of SEL.
BROWSE SEL BOT	Browse to bottom of SEL.
BROWSE SEL FIND xxx	Browse forward to find string xxx in SEL.
BROWSE SEL BFIND xxx	Browse backward to find string xxx in SEL.
CHG EDT NORMAL	Use Event Default Table (EDT) default severities.
CHG EDT INFO	Override EDT; use INFO as default severity for all events except those specified in Event Preference Table (EPT).
CHG EDT MINOR	Override EDT; use MINOR as default severity for all events except those specified in Event Preference Table (EPT).
CHG ELNK ACTIVE hostname	Set the system active Ethernet interface IP address.
CHG ELNK INACTIVE hostname	Set the system inactive Ethernet interface IP address.
CHG EPT aa... a INFO x	Change an Event Preference Table (EPT) entry to Information severity, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry

Table 40
Commands and Objects (Part 2 of 8)

=> **Command**	Description
CHG EPT aa... a EDT x	Change EPT to NT-defined severity from EDT, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry
CHG EPT aa... a MAJOR x	Change an EPT entry to Major severity, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry
CHG EPT aa... a MINOR x	Change an EPT entry to Minor severity, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry
CHG EPT aa... a CRITICAL x	Change an EPT entry to Critical severity, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry
CHG FMT_OUTPUT OFF	Turn off formatted output.
CHG FMT_OUTPUT ON	Turn on formatted output.

Table 40
Commands and Objects (Part 3 of 8)

=> **Command**	**Description**
CHG MASK nnn.nnn.nnn.nnn	Change subnet mask.
CHG PPP LOCAL hostname	Set the system local Point-to-Point Protocol interface IP address.
CHG PPP REMOTE hostname	Set the system remote Point-to-Point Protocol interface IP address.
CHG PTM 0-60	Change Point-to-Point Protocol idle timer to specified value (in minutes).
CHG SELSIZE 5-(500)-2000	Change System Event List Size (number of events in SEL).
CHG SUPPRESS 5-(15)-127	Change global suppress for events (number of occurrences before event is suppressed).
CHG TIMER (1)-60	Change global timer window length in minutes. See "Global Window Timer Length" on page 218 for more information.
NEW EPT aa... a INFO x	Assign Information severity to new EPT entry, where: aa... a = an event class with an event number (for example, BUG1000, ERR0025) x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry

Table 40
Commands and Objects (Part 4 of 8)

=> **Command**	Description
NEW EPT aa... a EDT x	Assign NT-defined severity from EDT to new EPT entry, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry
NEW EPT aa... a MAJOR x	Assign Major severity to new EPT entry, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry
NEW EPT aa... a MINOR x	Assign Minor severity to new EPT entry, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry
NEW EPT aa... a CRITICAL x	Assign Critical severity to new EPT entry, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
	x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or the **CHG SUPPRESS** entry

Table 40
Commands and Objects (Part 5 of 8)

=> **Command**	**Description**
NEW HOST hostname IP address	Configure a new host entry. The host name must exist in the host table.
	The default setting for the Primary IP address is: 137.135.128.253. The default setting for Primary Host Name is: PRIMARY_ENET.
	The default setting for the Secondary IP address is: 137.135.128.254. The default setting for the Secondary Host Name is: SECONDARY_ENET.
	Host Name Syntax: A host name can be up to 16 characters in length. The first character of a host name must be a letter of the alphabet. A character may be a letter, number, or underscore(_). A period is used as a delimiter between domain names. Spaces and tabs are not permitted. No distinction is made between upper and lower case.
NEW ROUTE network IP gateway	Configure a new routing entry.
OUT EPT aa... a	Delete a single Event Preference Table (EPT) events, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
OUT EPT ALL	Delete all entries in Event Default Table (EDT).
OUT HOST nnn	Delete configured host entry.
OUT ROUTE nn	Delete configured routing entry.

Table 40
Commands and Objects (Part 6 of 8)

=> **Command**	Description
PRT EDT aa... a	Print a single Event Default Table (EDT) event, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025)
PRT EDT aa... a bb...b	Print a range of Event Default Table (EDT) events, where:
	aa... a = first entry in EDT event range (for example, BUG1000, ERR0025)
	bb...b = last entry in EDT event range (for example, BUG1000, ERR0025)
PRT ELNK	Print active and inactive Ethernet interface IP addresses.
PRT EPT aa... a	Print a single Event Preference Table (EPT) entry, where:
	aa... a = an event class with an event number (for example, BUG1000, ERR0025).
PRT EPT aa... a bb...b	Print specific Event Preference Table (EPT) entry, where:
	aa... a = first entry in EPT event range (for example, BUG1000, ERR0025)
	bb...b = last entry in EPT event range (for example, BUG1000, ERR0025).
PRT EPT ALL	Print all entries in Event Preference Table (EPT).
PRT FMT_OUTPUT	Print formatted output string.
PRT HOST	Print network host table entries) information stored in database.
PRT MASK	Print subnet mask stored in database.
PRT OPEN_ALARM	Print open Simple Network Management Protocol. (SNMP) traps setting.

Table 40
Commands and Objects (Part 7 of 8)

=> **Command**	**Description**
PRT PPP	Print Point-to-point Protocol interface address(es).
PRT PTM	Print current Point-to-point Protocol idle timer settings.
PRT ROUTE	Print routing table entries) information stored in database.
PRT SEL nn	Print most recent record(s) in system event list, where: nn = 0-(20)-SELSIZE. For example, if nn = 50, the 50 most recent events in the system event list will be printed.
PRT SELSIZE	Print System Event List size.
PRT SUPPRESS	Print global suppress value.
PRT TIMER	Print global timer window length (in minutes). See "Global Window Timer Length" on page 218 for more information.
OUT EPT ALL	Delete all entries in Event Preference Table (EPT).
OUT EPT aa...a	Delete a single EPT entry, where: aa... a = first entry in EPT event range (for example, BUG1000, ERR0025).
RST ELNK ACTIVE	Reset the system active Ethernet interface IP address to default value.
RST ELNK INACTIVE	Reset the system inactive Ethernet interface IP address to default value.
RST MASK	Reset subnet mask to default.
RST PPP LOCAL	Reset local Point-to-point Protocol interface IP address to default value.
RST PPP REMOTE	Reset remote Point-to-point Protocol interface IP address to default value.

Table 40
Commands and Objects (Part 8 of 8)

=> **Command**	**Description**
RST PTM	Reset Point-to-point Protocol idle timer to default.
UPDATE DBS	Rebuild INET database and renumber host and route entry ID.

LD 117 – Maintenance Commands

Maintenance commands share the same entry format as Administration commands

Table 41
Maintenance commands (Part 1 of 2)

=> **Command**	**Description**
DIS HOST n	Remove a host from the run time host table, where: n = host entry number.
DIS PPP	Disable Point-to-point Protocol access (this enables PPPD).
DIS ROUTE n	Remove a route from the run time routing table, where: n = route entry number.
ENL HOST n	Add a host to run time host table, where: n = host entry number.
ENL PPP	Enable Point-to-point Protocol access (Enables PPPD command).
ENL ROUTE n	Add a route to run time routing table, where: n = route entry number.

Table 41
Maintenance commands (Part 2 of 2)

=> **Command**	**Description**
SET MASK	Set ELNK subnet mask to configured value.
SET OPEN_ALARM slot address	Add an SNMP (Simple Network Management Protocol) trap destination slot address from 0 to 7.
	The address format is: x.x.x.x. (TCP/IP)
	To clear slot, set address to 0.0.0.0.
STAT HOST	Display current runtime host table status.
STAT PPP	Show Point-to-point Protocol connection status.
STAT ROUTE	Display host and network routing table.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

With the exception of the Alarm Management Notification and Cleanup subfeatures, this feature is optional. It is a major enhancement to the existing Alarm Filtering (ALARM_FILTER) package 243.

Feature implementation

This feature uses LD 117 for configuration and administration.

LD 117 features a command line interface that is accessed by specifying the command to be performed, the object on which it is to be performed, and the configuration fields to be created or modified.On-line help is available for each command by specifying a question mark (?) after a specific command (CHG?).

Command example

```
>
>LD 117
-> CHG EPT BUG574 Major 5
```

Where:

- CHG: Command

- EPT: Object

- BUG574: Alarm

- Major: Severity

- 5: Escalation

LD 117 – Summary of commands (Part 1 of 2)

Prompt	Response	Description
****	Abort	Abort the overlay.
BROWSE	Browse	Browse an existing log.
CHG	Change	Change/modify configuration of objects.
NEW	New	Add configuration of a new object.

LD 117 – Summary of commands (Part 2 of 2)

Prompt	Response	Description
OUT	Out	Delete an existing object.
PRT	Print	Print configuration of an existing object.

LD 117 – Object summary

Prompt	Response	Description
ALL	Active Alarm List	List of currently active alarms.
AALSIZE	Active Alarm List size	Size of the Active Alarm List in terms of number of alarms.
EDT	Event Default Table	Table of event entries with associated severities.
EPT	Event Preference Table	Table of customer's event entries with associated severities.
FMT_OUTPUT	Formatted Output	An option to output system events using a special forma.t
SELOGIZE	System Event Log Size	Size of System Event log in terms of number of events.
SELOG	System Event Log	A log of system events.
SUPPRESS	Suppress Count	Number of times same event is "processed" before it is suppressed.
TIMER	Global Timer Window	Global timer window length in terms of number of minutes.

LD 117 – Object fields summary for OUT command.

Object	Associated Fields	Field's Valid Inputs-Range	Description
EPT	EPT_ENTRY	ALL aa.a	Delete all entries EPT. Delete a single EPT entry (for example, BUG100).

LD 117 – Object fields summary for BROWSE command

Object	Associated Fields)	Field's Valid Inputs-Range	Description
SELOG	COMMAND	Up n	Traverse up n number of lines in System Event Log.
		DOWN n	Traverse down n number of lines in System Event Log.
		TOP	Traverse to top of System Event Log.
		BOT	Traverse to bottom of System Event Log.
		FIND xxx	Forward find string xxx in System Event Log.
		BFIND xxx	Backward find string xxx in System Event Log.
		TOP	Traverse to top of System Event Log.

LD 17 – Object fields summary for CHG command.

Object	Associated Fields	Field's Valid Inputs - Range	Description
AALSIZE	SIZE	0–(100) –500	Size in terms of number of alarm records.
EPT	EPT_ENTRY	aa.a	Event entry is considered of an event class with an event number (for example, BUG 100, ERR25).
	SEVERITY	(INFO),	Info severity
		EDT,	Use severity in EDT
		MAJOR,	Major severity
		MINOR,	Minor severity
		CRITICAL	Critical severity
	ESCALATE	(0)–SUPPRESS	Escalation value (has to be less than SUPPRESS value)
FMT_OUTPUT	SETTIING	(OFF) ON	Turn off formatted output. Turn on formatted output.
SIZE	SIZE	0–(1000)–3000	Size of System Event Log in terms of number of events.
SUPPRESS	COUNT	0–(15)–127	Number of occurrences before event is suppressed.
TIMER	LENGTH	(1)–60	Timer window length in minutes.

LD 117 – Object fields summary for NEW command.

Object	Associated Fields	Field's Valid Inputs Range	Description
EPT	EPT_ENTRY	aa.a	Event consists of an event calls and an event number (for example, BUG100, ERR25).
	SEVERITY	(INFO),	Info severity
		EDT,	Use severity in EDT
		MAJOR,	Major severity
		MINOR,	Minor severity
		CRITICAL	Critical severity
	ESCALATE	(0)–SUPPRESS	Escalation value (has to be less than SUPPRESS value)

LD 117 – Object fields summary for PRT command.

Object	Associated Fields	Field's Valid Inputs - Range	Description
AAL	RECORDS	0–(20)–AALSIZE	Number of alarm records to be printed.
AALSIZE	Not applicable.		
EDT	ENTRY_MIN	ALL	Print all entries in EDT.
		aa..a	Event range minimum
EPT	EPT_ENTRY	AAL	Print all entries in EPT.
		aa.a	Event entry consists of an event class with an event number (for example, BUG100, ERR25).
FMT_OUTPUT	SETTING	(OFF) ON	Turn off formatted output. Turn on formatted output.
SELOGSIZE	Not applicable.		
SUPPRESS	Not applicable.		
TIMER	Not applicable.		

LD 17

Alarm filtering

An alarm is a system message that takes the form of ABCDxxxx, where ABCD is the class mnemonic and xxxx is the unique three- or four-digit message code.

A *system alarm* is an alarm that is not the direct result of operator actions, such as a message that is sent when an overlay runs during midnight processing.

An *overlay alarm* is an alarm that results from an operator's interaction with an overlay, such as an invalid response to a prompt.

With alarm filtering, the user can configure a system terminal to receive filtered system alarms. For example, a terminal can be configured to receive only those system alarms that require intervention. Other system alarms can be stored in the History File. Alarm filtering can be enabled or disabled on a per system basis.

Alarm filtering is controlled by the contents of the Alarm Filter Table, configured in LD 17 and printed in LD 22. The Alarm Filter Table consists of the Alarm Filter List and the Exception List; a default table is provided. Errors that match an entry in the Alarm Filter List and *not* in the Exception List are sent to the system terminal.

For example, the Alarm Filter List might include CED+++, indicating that all CED alarms are sent to the terminal. However, if the Exception List includes CED000, then CED000 alarms are not sent.

Operating parameters

Only system alarms can be filtered. Traffic messages and overlay alarms, as well as SYSxxx and INIxxx messages, cannot be filtered.

The maximum number of entries in the Alarm Filter Table is 50 alarms and 50 exceptions.

Filtered output contains only the first line of the system message.

After a system reload, the system time and date must be reconfigured. If they are not, the time and date stamps for system alarms will be incorrect.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

Alarm Filtering (ALRM_FILTER) is available as package 243. It requires the History File (HIST) package 55.

Feature implementation

Use LD 17 to define alarm filters and exceptions for each system basis.

LD 17 – Configure Alarm and Exceptions Filter data. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change
TYPE	ALARM	Access the default Alarm Filter Table; system responds by displaying the current settings for the Formatted Output and Alarm Filter options: FMT_OUTPUT (aaaa) AF_STATUS (bbbb)
FMT_OUTPUT	ON (OFF) <cr>	Enable Formatted Output printing Disable Formatted Output printing Retain current setting
AF_STATUS	ON (OFF) <cr>	Enable Alarm and Exception Filtering Disable Alarm and Exception Filtering Retain current setting
A_FILTER	NEW CHG OUT X <CR>	Add Change Remove an existing entry Remove an existing entry Exit Alarm Filter entry
TRIGGER	aa...aa <cr>	Enter string of up to 10 characters (containing at least one alphanumeric character and optionally the plus sign [+] as a wild card) that identifies an alarm type that is to be filtered. Retain the current value for this parameter.

LD 17 – Configure Alarm and Exceptions Filter data. (Part 2 of 2)

Prompt	Response	Description
SEVERITY		Identify the severity of the alarm type to be filtered:
	Critical	Conditions that threaten operational status
	Major	Serious but operational conditions
	Minor	Other error conditions
	(None)	Conditions with no severity rating
	<cr>	Retain the current value for this parameter
SUPPRESS	0–(5)–127	Enter the number of times an alarm can occur within a 24-hour period before it is suppressed; 0 disables suppression.
ESCALATE	0–(2)–127	Enter the number of times a major alarm can occur before it is escalated to critical; 0 disables escalation
A_FILTER	<cr>	Exit Alarm Filter entry
E_FILTER	NEW	Add Exception entry
	OUT	Remove an existing entry
	X	Remove an existing entry
	<cr>	Exit Exception entry
TRIGGER	aa...aa	Enter a string of up to 10 characters (containing at least one alphanumeric character and optionally the plus sign [+] as a wild card) that identifies an alarm that is NOT to be filtered.
E_FILTER	<cr>	Exit Exception entry

Each entry in the Alarm Filter List includes the following information:

- **Trigger** – Triggers are alarm identifiers, and in both the Alarm Filter List and the Exception List take the form ABCDxxxx, where ABCD is the message mnemonic and xxxx is the specific message identifier. The plus sign (+) is a wild card character that can be used in the message identifier.

  For example, an entry of DTI++++ in the Alarm Filter List causes all DTI messages to be filtered (unless there is a related entry in the Exception List). The wild card character cannot be used in the mnemonic portion of

the list entry. For example, B+++++++ is an invalid entry because B is not a valid mnemonic.

The valid message mnemonics appear in Table 42.

Table 42
Valid mnemonics for the Alarm Filter List

Mnemonics:					
ACD	CDM	DTA	LNK	OVL	TFN
ADD	CED	DTC	MFR	PCH *	TRK
AMH	CIOD*	DTI	MFS	PMS	TSM
AMLM	CMON *	DTRK	MISP	PRI	TTY
ATM	CNF	EDD	MSDL	PWR	VAS
AUD	CNI *	EHM	MWL	RPD	XCT
AUTH	CSA	ERR	NACD	RPL	XMI
BERR *	CSC	ESDA	NCT	RPT	
BIC	DBMT *	ESDI	NPR	SCSI *	
BSD	DCH	HWI *	NWS	SDL	
BUG	DLO *	IOD	OSM *	TDS	
CCED *	DSET	ISR	OVD	TEMU	
* Applies to only Large Systems					

- **Severity Level** – The four severity levels, from least to most severe, are None, Minor, Major, and Critical. See SEVERITY in "Use LD 17 to define alarm filters and exceptions for each system basis." on , for a description of each severity. The severity level is used for output formatting and for potential escalation from Major to Critical. See ESCALATE in "Use LD 17 to define alarm filters and exceptions for each system basis." on .

- • **Suppress Threshold** – This threshold specifies the number of times an error can occur in a 24-hour period before it is suppressed. Using this threshold can reduce the number of redundant messages that appear at the terminal.

- • **Escalate Threshold** – For Major alarms only, this value indicates the number of times an alarm can occur before it is escalated from Major to Critical.

Each alarm has an associated counter that increments with each occurrence of the alarm and is reset as part of the daily routines. The Alarm Summary Report displays the status of these counters, which is an indication of the general stability of the system.

Exception Filter List

The Exception Filter List is a list of specific alarm triggers, which are defined on .

TTY output device

When a terminal is assigned with a USER type of FIL in LD 17, it receives filtered alarm output. In addition, if it can load overlays, the terminal receives the normal communications from the overlay, including any SCH messages. However, it does *not* receive MTC, BUG, and CSC messages. See "LD 17 – Defining a terminal to receive filtered alarms" below to configure the terminal.

LD 17 – Define a terminal to receive filtered alarms. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action Device and Number

LD 17 – Define a terminal to receive filtered alarms. (Part 2 of 2)

ADAN	NEW CHG OUT <TTY PRT> 0–15	Add or change an I/O device TTY = Teletype port number PRT = Printer port number
USER	FIL	Allow only overlay and filtered alarm output, including critical alarms from auxiliary processors.

Output format for filtered alarms

All displayed system messages will appear in the following three-line format. The second and third lines are optional.

> <severity> <id> <time> <date> <seq no> <event> <type>
> <TAB> Operator data: <operator data>
> <TAB> Expert data: <expert data>

where:

<severity>	Alarm severity: *** indicates Critical ** indicates Major * indicates Minor (blank) indicates None
<id>	A unique identifier for the error, up to 10 characters, such as BUG3001
<date>	DD/MM/YY
<time>	HH:MM:SS
<seq no>	Sequence number of this alarm report
<event>	Event type: MSG indicates message (the default) SET indicates setting an alarm CLR indicates clearing an alarm
<TAB>	An 8-character indent
<operator data>	A 30-character field to help determine how to clear the fault
<expert data>	A 30-character field for use by a system expert for debugging

Feature operation

To request a printout of both the Alarm Filter List and the Exception List, use LD 22.

LD 22 – Print the Alarm Filter List and Exception List.

Prompt	Response	Description
REQ	PRT	Print
TYPE	ALARM	Print the Alarm Filter List followed by the Exception List

A sample of the output appears below. The "MAJOR+" in the second line of the Alarm Filter Summary indicates that the alarm was escalated to a CRITICAL severity.

```
FMT_OUTPUT: ON
AF_STATUS: ON

ALARM FILTER SUMMARY

TRIGGER     SEVERITY     SUPPRESS     ESCALATE
DCH+++      MAJOR        005          001
ERR+++      MAJOR+       005          001
MSDL+++     MAJOR        005          001

EXCEPTION FILTER SUMMARY
TRIGGER
DCH100
OVL003
```

To request a printout of the Alarm Summary information, use LD 2.

LD 2 – Print the Alarm Summary report.

Command	Description
ASUM	Print the Alarm Summary Report

A sample of the output produced appears below:

FMT_OUTPUT: ON
AF_STATUS: ON

ALARM FILTER SUMMARY

TRIGGER   SEVERITY   COUNT
DCH+++   MAJOR+   020
ERR+++   MAJOR+   020
MSDL+++   CRITICAL   001

EXCEPTION FILTER SUMMARY
TRIGGER
ERR020

Appendix A: 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 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 43 shows the name of serial ports on the Signaling Server.

Table 43
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 MS Windows nomenclature is used in this section.

Table 44 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 44
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 set 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 3
Setting the modem serial port speed for the Signaling Server

1   Log in to the OAM shell.

2   Issue the stty command and set the serial port speed of COM1 to
    38400 bps.

        oam> stty 38400

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 set the speed. Refer to the General tab of the Dialup
Networking Client properties; see Figure 13 on page 255.

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:

•   Send 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 45 on page 250.

Table 45
DIP switch settings (Part 1 of 2)

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

Table 45
DIP switch settings (Part 2 of 2)

DIP Switch	Position	Description
DIP Switch 4	Down (ON)	Modem suppresses display of result codes
DIP Switch 5	Up (OFF)	Modem answers if S0=1 or greater
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 you will connect to Signaling Server's COM1 port, you must:

1   Connect a terminal directly to the modem

2   Set DIP switch 8 DOWN (ON)

3   Power the modem OFF/ON.

The modem will now respond to the AT command set; however, type carefully as 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 4
Using the AT command set

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 to step 6. Read and follow the
    technical reference for the modem you are installing to configure it for
    Send Data hardware flow control only.

Configuring a Dial-up Networking PPP Client
for remote access to the Signaling Server

Use Procedure 5 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 5
Configuring a Dial-up Networking PPP client for remote access to the Signaling Server

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 selection **Properties**.

     The properties window for the newly created dial-up connection appears.
     The Properties window has five tabs (see Figure 12 on).
     Configure the properties as outlined in the following steps.

Figure 12
Dial-up connection - General tab
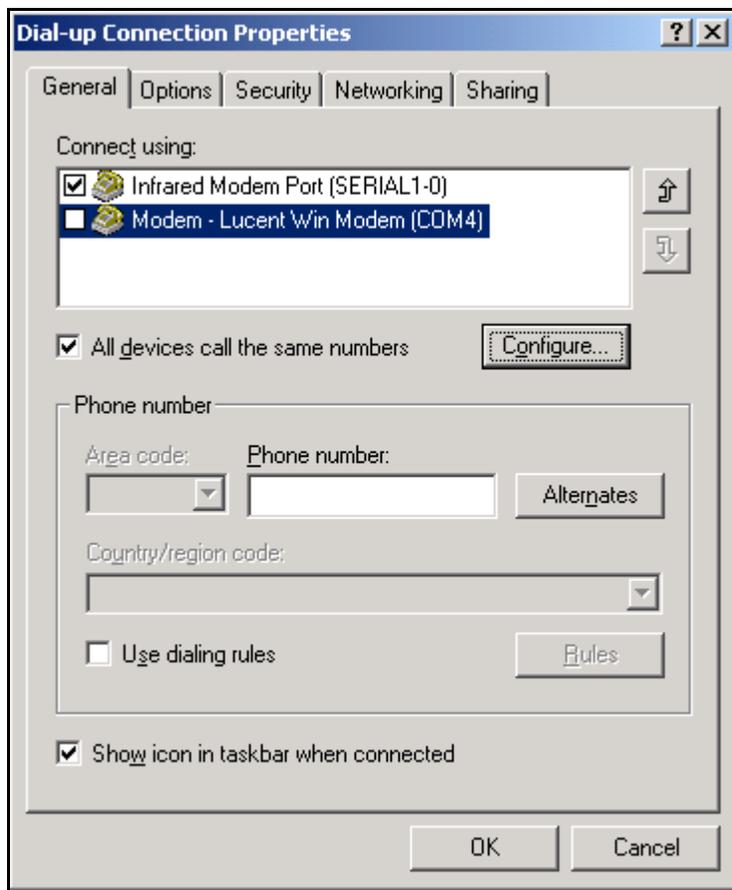
7   On the **General** tab, click the **Configure** button.

The **Modem Configuration** window opens (see Figure 13 on),

Figure 13
Modem Configuration
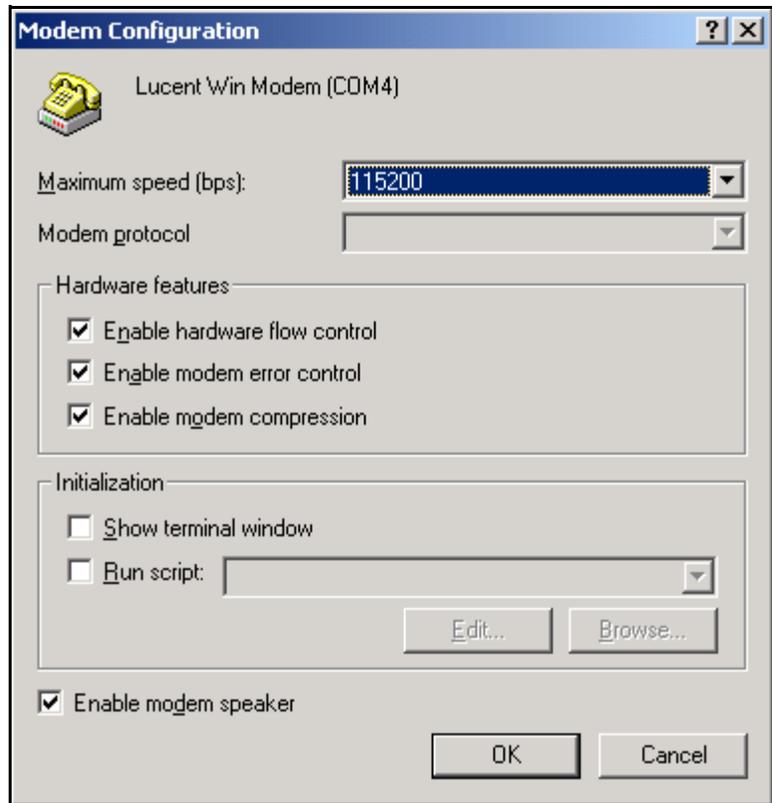
8   Set the following:

   a.   Set **Maximum speed (bps)** to 38400, 57600, or 115200.

   b.   Check **Enable hardware flow control**.

   c.   Check **Enable modem error control.**

   d.   Check **Enable modem data compression**.

   e.   Uncheck **Show terminal window**.

   f.   Uncheck **Run script**

    g.   Check **Enable modem speaker**.

    h.   Click **OK**. The Dial-up Connection window reappears.

9   Select the **Options** tab (see Figure 14 on).

Figure 14
Dial-up connection - Options tab
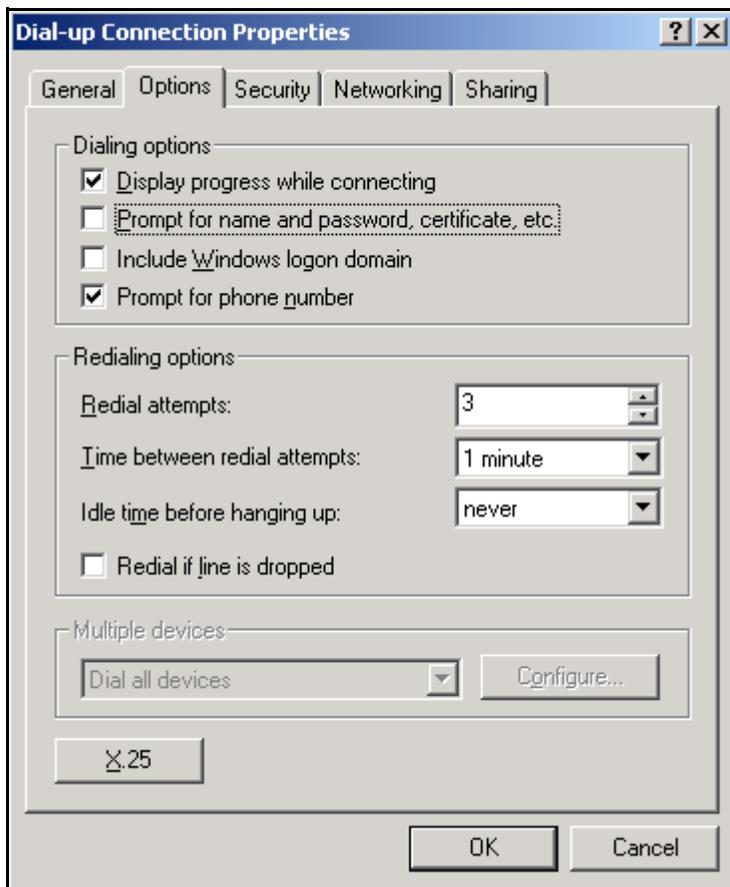
    a.   Enable **Display progress while connecting**.

    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 (see Figure 15 on).

Figure 15
Dial-up connection - Security tab
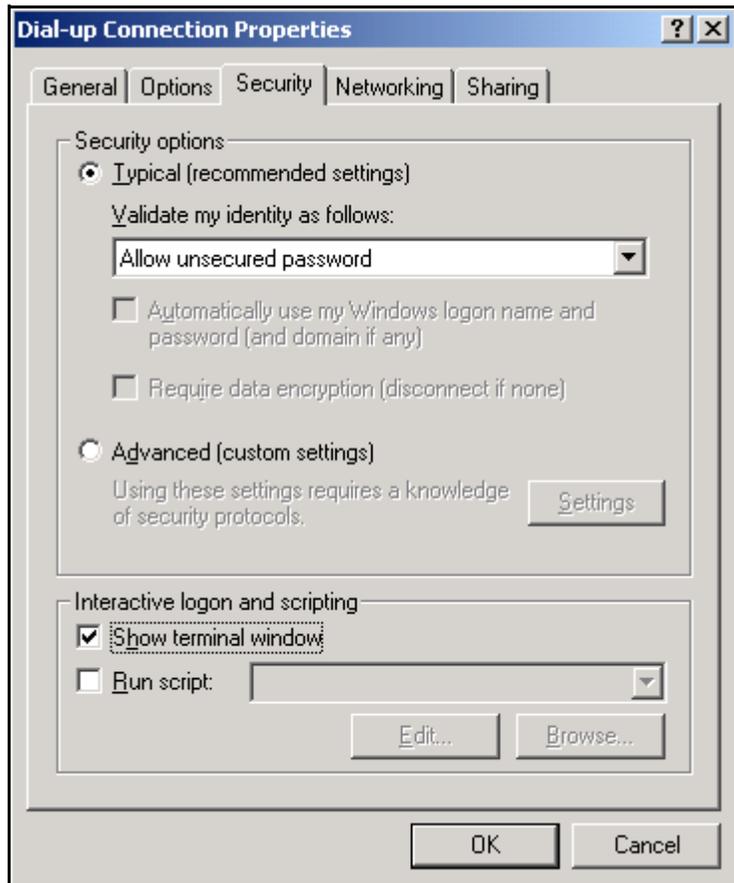
a. Under **Security options**, select **Typical (recommended settings)** radio button.

b. Under **Interactive logon and scripting**:

i. Enable **Show terminal window**.

ii. Ensure that **Run script** is not checked.

11 Select the **Networking** tab (see Figure 16 on page 258).

Figure 16
Dial-up connection - Networking tab
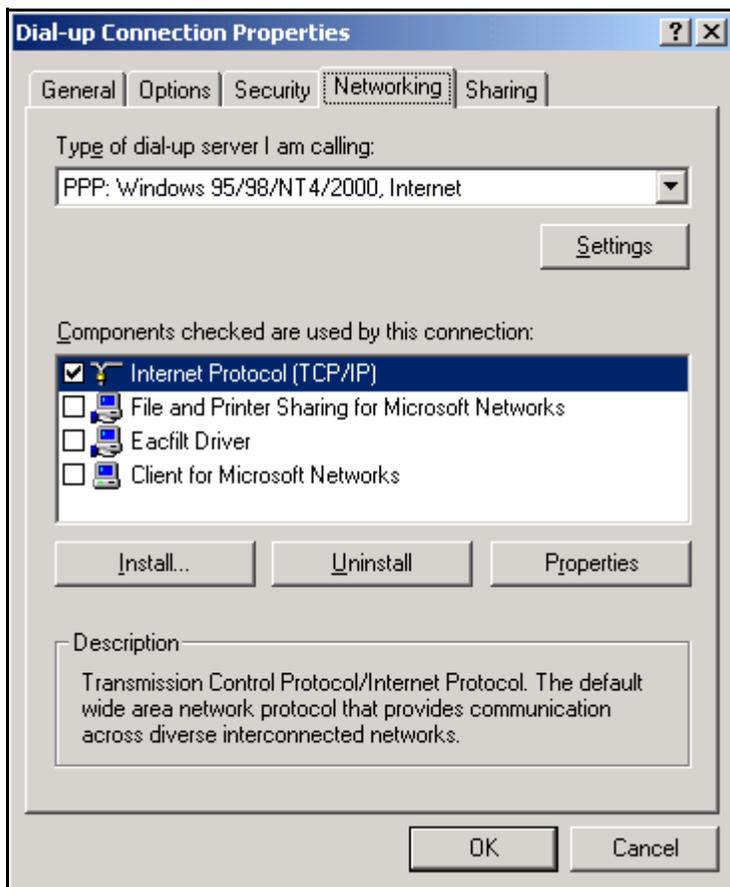
    a.   Under **Type of dialup server I am calling:,** select PPP, Windows 95/98/NT4/2000, Internet.

    b.   Click the **Settings** button. The PPP Setting window opens (see Figure 17 on).

Figure 17
PPP Settings
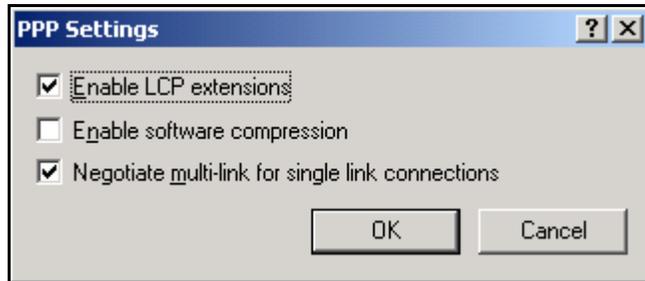
    i.   Uncheck the **Enable software compression** checkbox.

    ii.   Click **OK** to close the PPP Settings window.

    c.   Under **Components used by this connection**:

    i.   Enable **Internet Protocol (TCP/IP)**.

    ii.   Disable **File and Printer Sharing for Microsoft Networks**.

    iii.   Disable **Client for Microsoft Networks**.

    iv.   Disable any other components.

    d.   Highlight Internet Protocol (TCP/IP) and click the **Properties** button.

The Internet Protocol (TCP/IP) Properties window opens (see Figure 18 on).

Figure 18
Internet Protocol (TCP/IP) Properties
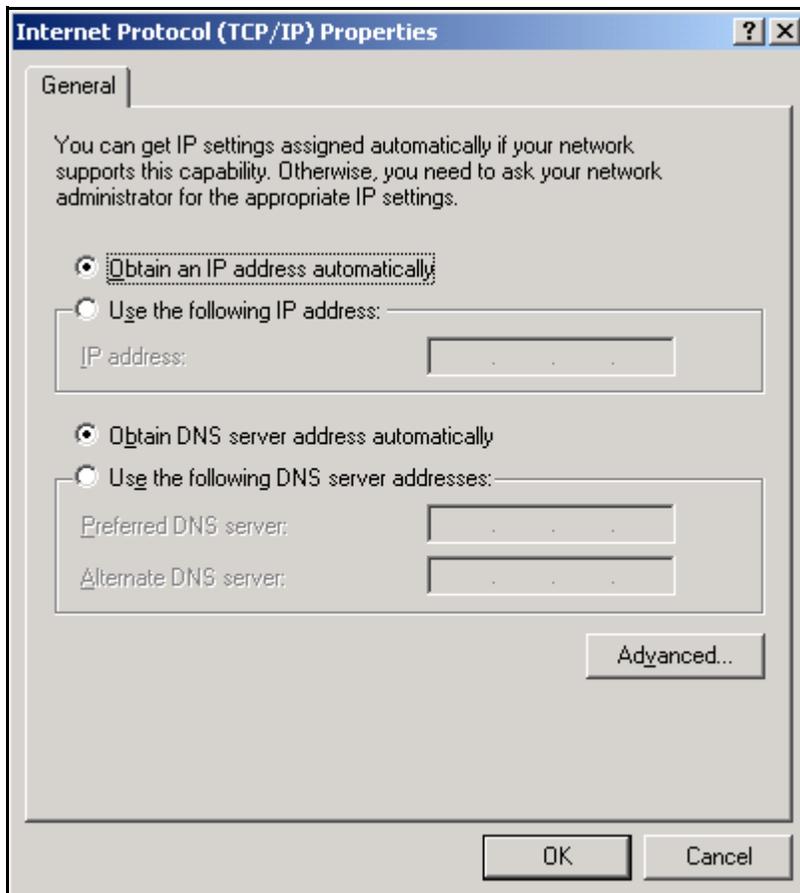
- i.   Select the **Obtain IP address automatically** radio button.

- ii. Select the **Obtain DNS server address automatically** radio button.

- e.   Click the **Advanced** button.

     The **Advanced TCP/IP Properties** window opens (see Figure 19).

Figure 19
Advance TCP/IP Properties - General tab
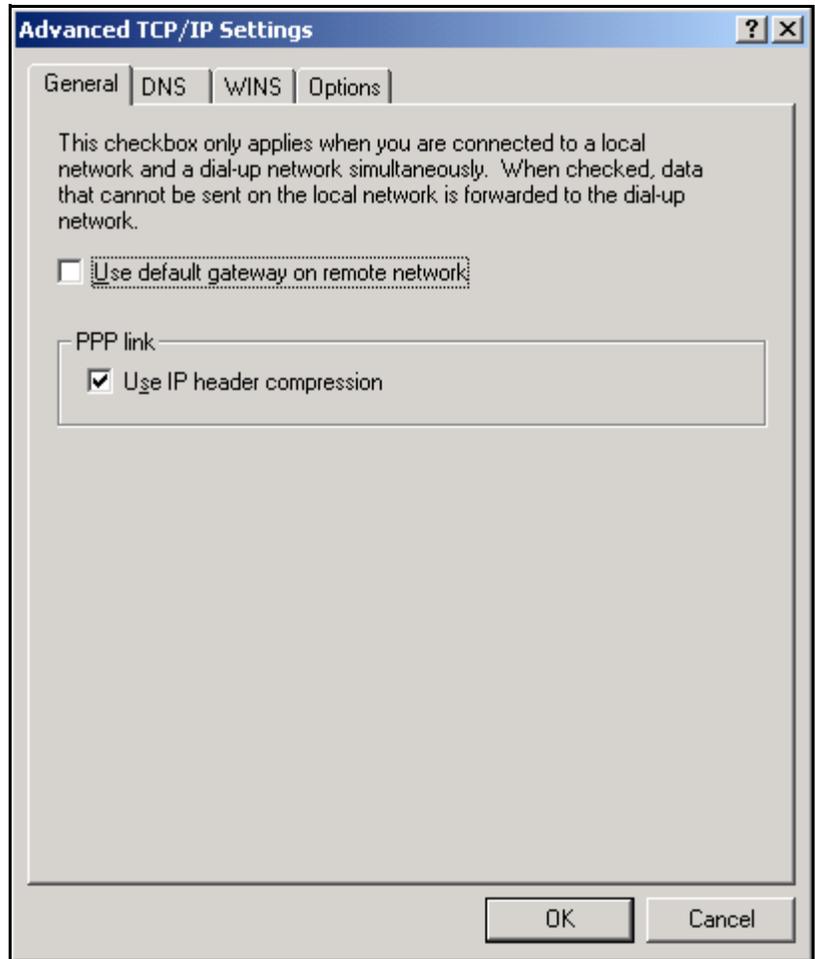
f. On the **General** tab:

    i.   Disable **Use default gateway on remote network.**

    ii. Enable **Use IP header compression**.

g.   Select the **Options** tab (see Figure 20):

Figure 20
Advance TCP/IP Settings - Options Tab
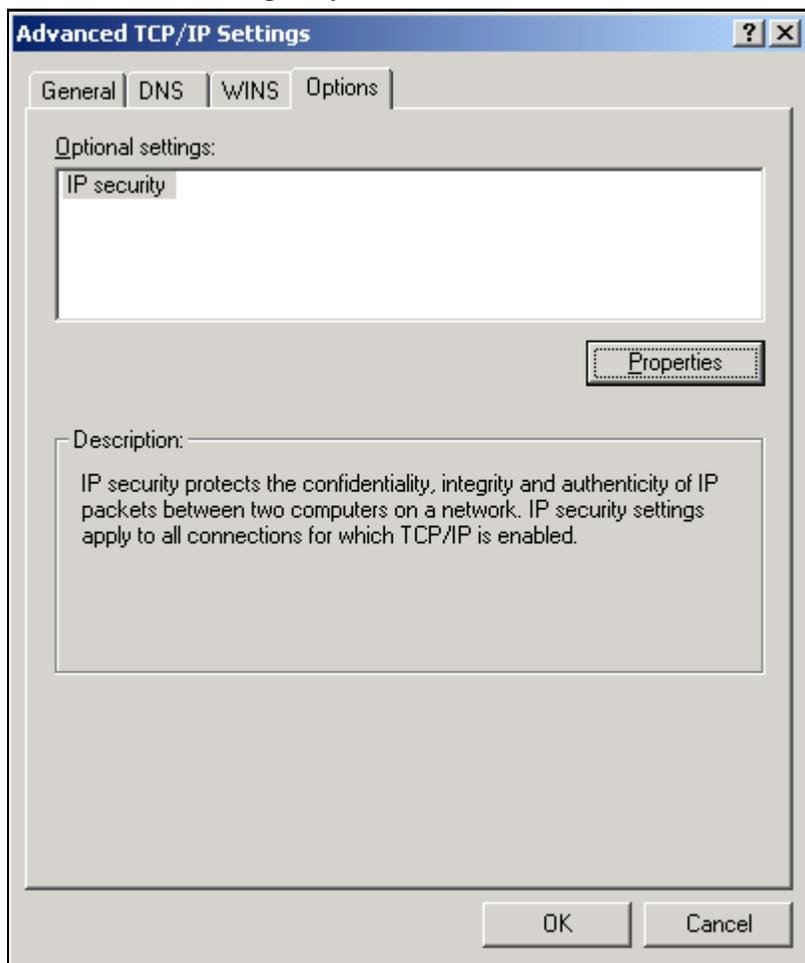
    i.   Click the **Properties** button. The **IP Security** window opens (see Figure 21).

Figure 21
IP Security
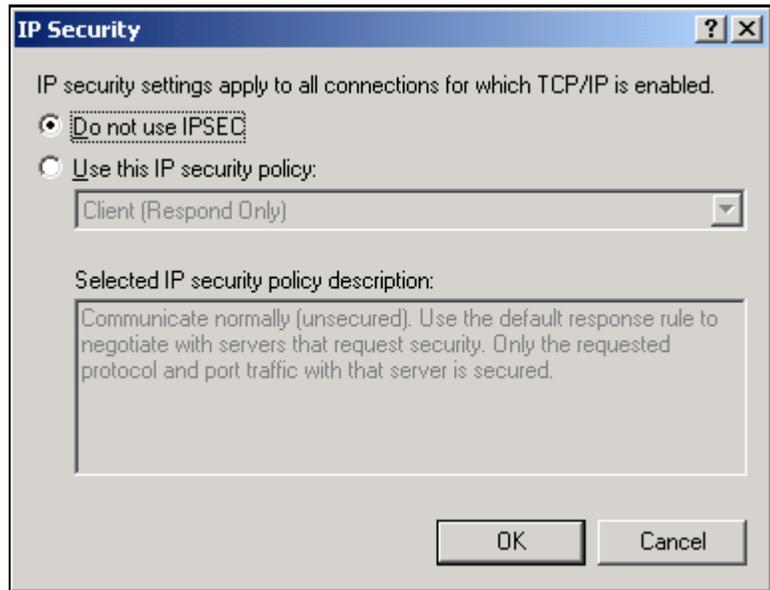
h.   Check the **Do not use IPSEC** radio button.

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.

Configure the Call Server route

Use Procedure 6 to configure the Call Server route for remote single point of access using the Signaling Server PPP link.

Procedure 6
Configure the Call Server route

1   Log in to LD 117.

2   Issue the following command:

   NEW ROUTE <Signaling Server's ELAN 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 IP Address>.

Configure Voice Gateway Media Card ELAN route

Configure Voice Gateway Media Card ELAN route for remote single point of access using the Signaling Server PPP link.

Procedure 7
Configure the Voice Gateway Media Card ELAN route

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's ELAN 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 <SS ELAN IP Address>.

Use remote single point of access

Use Procedure 8 for remote single point of access using the Signaling Server PPP link.

Procedure 8
Using Remote Single Point of Access

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 46 shows the result of entering the ppp command.

Table 46
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 on 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.

When you exit the secondary rlogin or Telnet session, you will revert 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 the Signaling Server ppp3 local IP address.

4   Use the **IPInfoShow** command to get the ELAN network ID and subnet mask of the Signaling Server:

    oam> IPInfoShow

The ELAN network id is the Destination of the NET ROUTE entry that shows the Signaling Server ELAN IP address as the Gateway.

5   Write down the Signaling Server ELAN network ID and subnet mask.

6   Open a command window on the remote PC.

7   Enter the following command to add an IP route to the ELAN network ID by the Gateway of the PPP interface IP address of the remote PC (that is, the Signaling Server ppp3 Remote IP address).

    oam> route add <Signaling Server ELAN network ID> mask <Signaling Server ELAN 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 SS ELAN by the PPP interface is automatically removed from the remote PC's IP route table whenever the PPP link is disconnected.

8   Open a web browser on the remote PC and enter the URL of the Succession 1000 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 Gatekeeper on the same Signaling Server, you can point the web browser to the Gatekeeper web pages in the Element Manager web server on the PPP IP address 137.135.3.1/gk.

10 Once you have:

- created HOST ROUTE entries to Destination 137.135.3.2 by the Signaling Server ELAN IP address Gateway on each of the system elements, and

- added the route to the Signaling Server ELAN Destination 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.

To do this, click **Status | IP Telephony | Node** and then click the **Telnet via ELAN** button.

11 Establish a direct rlogin connection from the remote PC to the Call Server using the Signaling Server ELAN.

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.

Benchmarking

Benchmarks for Element Manager page loading time

Table 47 benchmarks for Element Manager page loading time at 38400 bps over a 33.6 kbps modem connection.

Table 47
Element Manager benchmarks

From	To	Time
Login page	Nortel Networks logo	12 seconds
Login page	Navigation tree (without control objects) ***Note:*** The Navigation Tree can be used immediately.	18 seconds
Login page	System Information display and Navigation Tree control objects for System Status and Configuration	26 seconds
Login page	Navigation Tree (with all control objects)	44 seconds
Configuration | IP Telephony pages	Node Summary page	15 seconds
Node Summary	Open a select node for editing	18 seconds

Benchmarks for File Transfer time

Table 48 shows the benchmarks for file transfer time at 38400 bps over a 33.6 kbps modem connection. The benchmarks were performed using FTP from a remote PC to the Signaling Server.

Table 48
File Transfer benchmarks

Action	Amount of data	Time	Rate
Puts	1554216 bytes	466.61 seconds	3.33 Kbytes/sec
Gets	1554216 bytes	420.40 seconds	3.70 Kbytes/sec

Meridian 1, Succession 1000,
Succession 1000M
System Management

**NORTEL
NETWORKS** ™