Meridian 1 and Succession Communication Server for Enterprise 1000

System Management

Document Number: 553-3001-300
Document Release: Standard 6.00
Date: January 2002

Printed in Canada

Revision history

January 2002

Standard 6.00. This document is up-issued to include content changes for Meridian 1 Internet Enabled Release 25.40 and Succession Communication Server for Enterprise 1000 systems.

April 2000

Standard 5.00. This is a global document and is up-issued for X11 Release 25.0x.

August 1996

Standard 4.00 for X11 Release 22.0x.

July 1995

Standard 3.00. This document is issued to indicate X11 Release 21 changes.

December 1994

Standard 2.00. Includes X11 Release 20 changes, and editorial changes.

December 1989

Standard 1.00. Includes updates and changes due to the introduction of new overlay 117.

Contents

About this document

This document applies to Meridian 1 Internet Enabled and Succession Communication Server for Enterprise 1000 systems.

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

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

Other documentation

Refer to the following Nortel Networks Technical Publications (NTPs) related to system management:

- *System Overview* (553-3001-100)
- *System Installation Procedures* (553-3001-210)
- *System Management Applications* (553-3001-301)
- *Features and Services* (553-3001-306)

- *Software Input/Output Guide Administration* (553-3001-311)
- *General Maintenance Information* (553-3001-500)
- *System Security Management* (553-3001-302)

System management overview

Contents

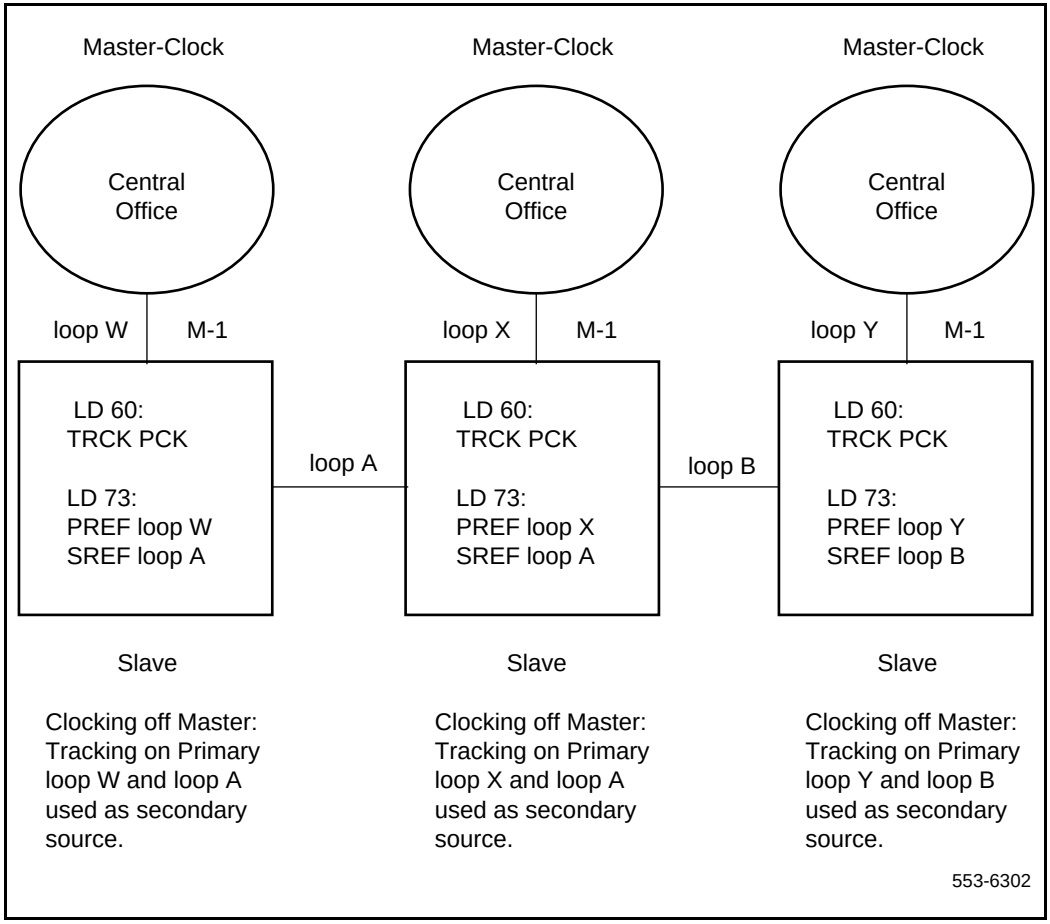
This section contains information on the following topics:

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. This document is intended to help system administrators and technicians gain that perspective.

I/O architecture

Figure 1 on page 10 identifies major elements in the system I/O architecture.

Figure 1
I/O architecture



System architecture

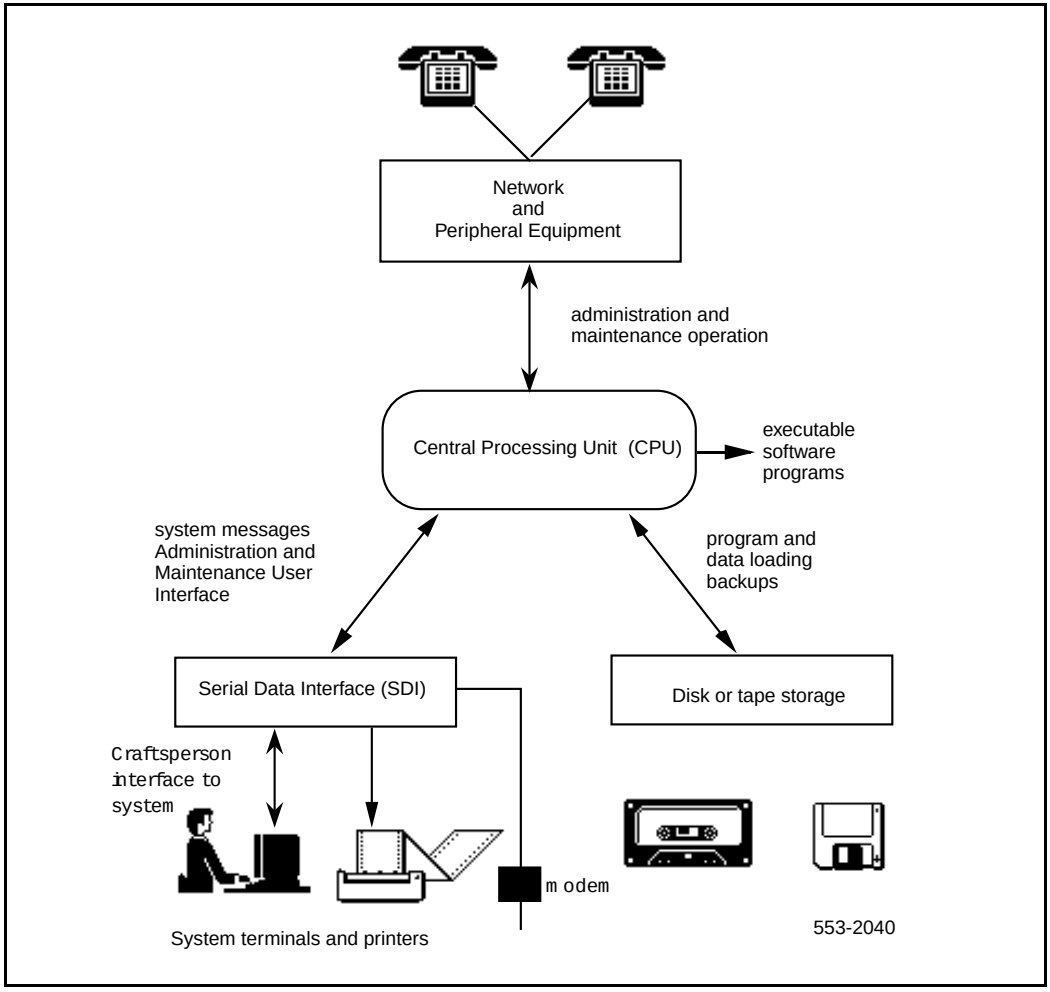
The system software provides call processing and feature operation, administration and system management programs, and maintenance and diagnostic programs.

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 page 12.

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 may 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 nonvolatile memory and resides on a field-replaceable board on the CPU. It includes various system control programs. Software releases and system types require different ROMs.

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 SYNC 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 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.

Communicating with the system

Contents

This section contains information on the following topics:

Reference list

The following are the references in this section:

- *System Management Applications* (553-3001-301)
- *Features and Services* (553-3001-306)
- *Administration* (553-3001-311)
- *Maintenance* (553-3001-511)

Introduction

System administrators communicate with the system using Input/Output (I/O) devices such as Video Display Terminals (VDTs), telephones, and printers (PRTs). These devices may be local (on-site) or remote. This section describes what devices are supported, how a system administrator logs in and out, and how administrative and maintenance programs operate.

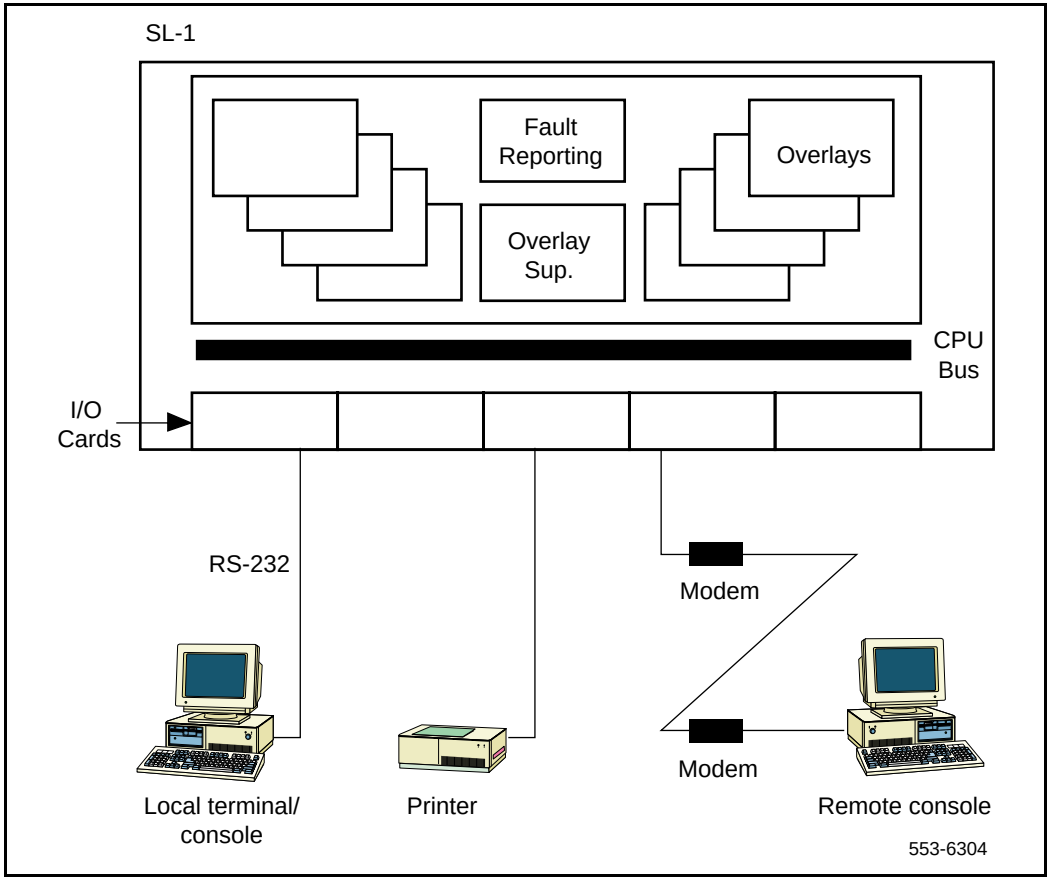
Multi-User Login enables up to five users (in addition to a background routine) to perform tasks concurrently. For more information, see "Multi-user considerations" on page 60, and "Multi-User Login" on page 79. See also "Multi-User Login" in *Features and Services* (553-3001-306).

Local and remote access

Devices used to control the system connect through serial data interfaces located in the central control unit. Serial data interfaces include SDI, MSDL, and ISDN D-Channel Interface Asynchronous Port.

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. See Figure 3 on page 20.

Figure 3
Local and remote devices



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.

PPP Access

The systems have Ethernet ports and support TCP/IP protocol stack using Point-to-Point (PPP). PPP is an asychronous 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 retard or 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 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. Here are the required configurations for the system:

- Baud rate is limited to the type of hardware 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 needs to 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 can not 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 links 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 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.
- 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 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.

PPP link establishment

A physical serial connection must exist before the PPP protocol can start up the link establishment process. The physical serial connection can be a direct line connection or through a modem dial up connection, and the PPP links can run on any active TTY port with MTC and SCH user type. For an in-bound link establishment, the following states must be completed:

- The physical serial link must be connected through a direct line or modem connection

- The PPPD command must be issued at the overlay supervisor prompt to start up the PPP session on the system
- The remote client system must start up its PPP session
- The two end-points must start up LCP
- The NCP must start up. The NCP is limited to TCP/IP network protocol
- PPP links are established and in operation

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 needs to 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

Table 1 lists the commands associated with a service change.

Table 1
SMP Overlay 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.
=>	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.

Table 1
SMP Overlay 117 Service Change (Part 2 of 2)

Prompt	Response	Description
=>	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 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 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 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 interfaces addresses and local and/or remote PPP interface addresses.
- For duel CPU setup, obtain two valid Ethernet interface IP addresses.
- Configure 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 address through LD 117 "NEW HOST."

- Make sure 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 may need. 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 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 idle timer in LD 117 with ‘CHG PTM nnn”.

SDI configurations

Any system SDI port configured as MTC and/or SCH with other user types can be used to establish a PPP connection.

Modem configuration

Since the system SDI ports do not monitor the RS-232 data leads, the modem connected to the SDI port must be pre-configured for proper operation.

Most of the system SDI ports, except MSDL SDI, are set up as a DCE for a terminal connection. When connecting N1 SDI to a modem, (another DCE), a null modem adapter is required.

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 baudrate.

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 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 VxWork OS, some of the services may allow unauthorized access to system data. Table 2 lists the services available.

Table 2
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 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 Network-managed products.

Affected components

Table 3
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, 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-set both IOP's 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 set. 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.

IOP Configuration

Every 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 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 should 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 Local Area Network Controller for Ethernet (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 Local Area Network Controller for Ethernet (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 the code for it 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 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 (PPP) support

For remote access to and from the system, PPP is supported. Refer to the previous PPP section.

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 at 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 4.

Table 4
Default IP Address and Host Name

Field	Default Setting
Primary IP address	137.135.128.253
Primary Hist 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 3 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 system when power fails on CPU, hardware-sanity watchdog-timer-time-out.

- Manual (forced) switchover by command ‘SCPU’ in LD 135.
- Hardware (forced) switchover by the technician by turning the switch on the CP card to 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 cam 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 CP card side 0 and side 1 are both in 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 normal position
- Boot-up system in redundancy mode by a technician

Table 5 summarizes the possible states of a redundant system and the state of the Ethernet connection being used.

Table 5
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 (IOP) 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 become 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 Ethernet link as described below:

1 **Maintenance** – to conform with the design of existing overlay, any maintenance error message related to LANCE will be composed of CIOD and an error code.

2 **Administration** – any administration error will be in SCH format.

3 **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 6 on page 44 illustrates how to change the host name and IP address for Primary and Secondary CPU side. Refer to "Direct Gateway Access" on page 58.

Ethernet configuration

Table 6 shows the prompt sequence and responses for configuring the Ethernet link in LD 117.

Table 6
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 7
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 8
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:

- the 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 VDT or a 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 9.

Table 9
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 10.

Table 10
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:
  - an RS-232-C compatible Video Display Terminal (VDT), referred to as a system terminal
  - a PC with a serial port
  - an attendant console
  - an RS-232-C compatible Teletypewriter (TTY)

  - a VT100 TTY type interface
  - a VT220 with 7-bit or 8-bit mode with access to subsystems through STA using MDSL

- input only:
  - a 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:
  - An 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.

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.

Use Procedure 1 on page 49 to log into the system from a VDT. Use Procedure 2 on page 50 to log into the system from a maintenance telephone.

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 into 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 *System Messages Guide* (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 *System Messages Guide* (553-3001-411).

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

LD xx <cr>
–**or**–
LD xxx <cr>
–**or**–
LD xx D <cr>

where xx or xxx is the number of the program; D forces a load from disk. (D applies only to non-Option 81C systems equipped with Overlay Cache Memory.)

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

Table 11
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 3.

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:

****

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 12 on page 54 shows an example of a command recognized by several different maintenance programs.

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

Table 12
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 13 on page 55 shows an example of how to use an administration program.

Table 13
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 *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}
–**or**–
LD xx D <cr> {for Attendant Administration}

where xx or xxx is the number of the program; D forces a load from disk. (D applies only to non-Option 81C systems equipped with Overlay Cache Memory.)

Overlay characteristics

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

Data groups and gateway prompts

An individual prompt can be accessed via a special gateway prompt to its data group. For example, PWD is the LD 17 gateway prompt to prompts related to passwords. See sample gateway prompts in Table 14.

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

By entering a gateway mnemonic in response to the TYPE prompt in LD 17, the user gains access to its data group. See *Administration* (553-3001-311) for further detail.

Table 14
Sample gateway 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
Note: Prompts in LD 17 not belonging to any other data group are part of the PARM data group. These prompts include CSQI, CSQO, AXQI, AXQO, FRPT, MANU, CLID, MGCR, DCUS, MAGT, MSCL.	

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 15
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 Overlays 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 *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 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 dis 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 16 shows some examples of the linked programs.

Table 16
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 on all C processor systems (options 11C, 51C, 61C, 81 and 81C). This utility 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" in *System Management Applications* (553-3001-301).

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 Overlays 10 and 11. Also multiple copies of print Overlays 20, 21, 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” and “Single Terminal Access” in *System Management Applications* (553-3001-301).

Using programs

Special characters

The characters shown in the following table have a special meaning to the software.

Table 17
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” in *System Management Applications* (553-3001-301) 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. Refer to *System Management Applications* (553-3001-301) for more information

Printing

Table 18 lists the print programs and the type of data they can print.

Table 18
Print programs and 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
21	ATM routes ATM schedules CAS key Code Restriction data Customer Data Block Route data Set relocation data Trunk members
22	Audit trail for Limited Access to Overlays Configuration Record Code inventory for Option 81C 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
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 page 56.

For information on messages that may appear during program execution, see “System messages” on page 68.

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:

1 **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.

2 **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".

3 **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.

4 **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.

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

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. The System Event List survives Sysload, Initialization and power failures.

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:

1 **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 19
Sample Event Default Table (EDT)

Error Code	Severity
ERR220	Critical
IOD6	Critical
BUG4001	MInor

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

2 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:

a. override the default event severity assigned by the default table

b. escalate event severity of frequently occurring minor or major alarms

Table 20
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. See section below for explanation of wildcard entries.

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 66 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.

Ethernet

LD 117 may be used to configure and manage an IP network interface. The system is hardware-equipped for this advance 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 an 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 (PIPA). A dual CPU system operating in split mode (the mode used only when upgrading software or hardware) uses the Secondary IP Address (SIPA).

Remote access

Remote access to system switches is made possible with Point-to-Point Protocol (PPP). LD 117 may be used to configure IP addresses for Point-to-Point Protocol. For more information, refer to LD 117 in the *Maintenance* (553-3001-511).

System reporting

Contents

This section contains information on the following topics:

Reference list

The following are the references in this section:

- *Software Input/Output Guide Administration* (553-3001-311)
- *General Maintenance Information* (553-3001-500)

The system provides comprehensive information to help monitor the system and diagnose problems. This section describes the more prominent mechanisms that enhance communication between the system and the administrator or technician.

Faceplate displays

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

LEDs

Many circuit cards have one or more LEDs on the faceplate. The LED 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 *General Maintenance Information* (553-3001-500).

Maintenance displays

Maintenance displays on Meridian 1 circuit cards present hexadecimal (text on Option 81C) 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. The most recent 16 codes displayed on a controller card remain in memory, where they can be viewed through LD 30. On an Option 81C, the most recent 64 codes displayed on a CP card remain in memory, where they can be viewed through LD 135.

To interpret maintenance display codes, refer to "HEX" in the *Software Input/Output Guide Administration* (553-3001-311).

System messages

System messages include status, error, and informational messages. These messages appear on appropriately configured VDT and TTY devices. Configure the system in LD 17 to tailor the volume and type of system messages that appear on a VDT or TTY.

System messages use one of the following formats:

AAAxxx
AAAAxxxx

AAA or AAAA are mnemonics that identify the program issuing the message or the message type. Typical message types include Service Change (SCH), maintenance (such as AML and ATM), traffic (such as TFS), and Call Detail Recording (CDR). The xxx or xxxx identifies the specific message.

In the following message:

PWR0014

PWR indicates a problem with system power or temperature; 0014 specifically indicates that the system monitor failed a self-test.

System messages have two formats depending on the Alarm-Format prompt in LD 17. Regardless of the formatting, the message identifiers are described above.

Table 21 shows the types of messages that go to TTYs configured in LD 17 with specific user types:

Table 21
User types and related message types

User Mnemonic	Description
AML	Application Module Link
BDCH	Backup primary D-channel
DCH	Primary D-channel
FDK	Floppy disk unit
FIL	Filtered alarm output
HDK	Hard disk unit
HST	History File
PRT	Printer port number
TTY	Teletype port number

For a description of all system messages, refer to the *Software Input/Output Guide Administration* (553-3001-311).

System messages can be written to the System History File, Traffic Log File, or TTY Log File, each of which is described below. These files provide an audit trail of system activity for later review and analysis.

System History File

The History File 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.

LD 22 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.

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

- maintenance messages, such as those for a disk/tape unit enable/disable
- 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 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.

A Multi-User Login feature introduces a TTY log file that can be used to distinguish archived TTY interactions for a particular user. A Traffic Log File can be configured to store traffic reports only. 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

This section contains information on the following topics:With the Multi-User Login feature enabled, the log files associated with system TTY terminals record messages relating to the following:

- service changes
- user invoked Maintenance operations
- traffic (user requested reports via LD 2)
- CDR activity
- software bugs

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

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 new 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 new System Event List survives Sysload, Initialization and power failures.

For more information on the new disk-based System Event List, refer to the section titled “LD 117” on page 63.

Traffic Log File

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

"%" can be wired off while viewing the Traffic Log File so that off-line traffic report processing programs can use the output without stripping the "%" character.

LAPW Audit Trail

If LAPW is configured, this is a file that can be viewed to show Logins, Logouts, and Overlay loading.

Security

Contents

This section contains information on the following topics:

Reference list

The following are the references in this section:

- *System Management Applications* (553-3001-301)
- *System Security Management* (553-3001-302)

Most telecommunications systems provide protection from unauthorized and fraudulent use. Systems control access to features and functions, as well as provide audit trails of user sessions. In addition, administrators and users establish and adhere to security practices appropriate to each unique system.

Extensive system-wide security features are provided to help detect and prevent possible unauthorized access to the system and to Meridian Mail. For a comprehensive treatment of system security, refer to *System Security Management* (553-3001-302).

Session security

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 informational messages. In addition, it lets the system administrator track sessions on a TTY where unusual login activities have occurred.

Basic passwords

Meridian 1 system software provides two types of passwords that allow access to database configuration and maintenance programs:

- Level 1 passwords (PWD1)
  These passwords provide general access to the system so that service personnel can perform administrative and maintenance tasks.
- Level 2 passwords (PWD2)
  These passwords provide controlled access to the System Configuration Record so that system administrators can change passwords and perform other tasks related to system.

The system administrator uses LD 17 to enter or change passwords. Good security practices include changing all passwords regularly. Valid passwords must:

- contain 4 to 16 characters
- be composed of digits 0 through 9, and characters A through Z

An administrator (who must be logged in with PWD2) can associate a user name with PWD1, PWD2, and the 100 limited access passwords. The user name can be up to 11 alphanumeric characters. The LNAME_OPTION in LD 17, which defaults to NO, must be set to YES to indicate that login names are required.

Limited access passwords

With the Limited Access to Overlays feature implemented, the system administrator can restrict user access to specific programs and data. Use LD 17 to define up to 100 login passwords in the configuration record, each with its own set of access restrictions. For more information, see “Limited Access to Overlays” on page 78 and in *System Management Applications* (553-3001-301).

Secure Data Password

This password limits the service change of Authcodes in LD 88.

System management applications

Contents

This section contains information on the following topics:

Reference list

The following are the references in this section:

- *System Management Applications* (553-3001-301)

This section provides a brief description of each system management application. For an in-depth discussion of these applications, refer to *System Management Applications* (553-3001-301).

System History File

The system writes messages to a System History File to reduce the need for on-site TTY facilities. The View History File (VHST) capability in LD 22 supports selective viewing and/or printing of History File and Traffic Log File content. More information on this application appears on page 70.

Limited Access to Overlays

Limited Access to Overlays lets the administrator restrict user access to specific programs and data. The administrator can define up to 100 login passwords in the Configuration Record (LD 17), each with its own set of access restrictions. For each of these Limited Access Passwords (LAPW), the restrictions can include:

- access to specific overlays
- modification of specific customer data
- access to specific tenant numbers
- access to Speed Call lists via the print routines in LD 20
- defined access to the Configuration Record (CFN) in LD 17
- defined access via the Print Only option

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

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. The SDI is composed of software components that reside on the Meridian 1 and the MSDL.

The MSDL SDI supports three asynchronous serial data applications: TTY, PRT, and 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 auto-recovery

The following capabilities, available on other cards that support SDI, are also available on the MSDL SDI:

- Interfaces to TTYs, printers, modems, and VDTs
- High Speed Link (HSL) for ACD
- Auxiliary Processor Link (APL) for ACD
- ACD Package C displays and reports
- CDR TTY
- System terminal
- Bug and error messages
- Overlay 2 and Traffic Measurements
- Filtered alarms
- Data administration

Fault Management

Fault management administration and maintenance is conducted in LD 117. This overlay is described on page 63. A more detailed description of this overlay can be found in *System Management Applications* (553-3001-301).

Multi-User Login

Meridian-1 Multi-User Login 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 the efficiency of craftspersons by enabling them to perform tasks in parallel. To facilitate this operating environment, Multi-User Login includes the following functionalities:

- database conflict prevention
- additional user commands

- TTY Log Files
- TTY directed I/O

Please refer to *System Management Applications* (553-3001-301) for more information.

Single Terminal Access

Single Terminal Access (STA), provides integrated access to Operations, Administration, and Management (OA&M) functions for the systems it monitors. It reduces the number of physical devices needed to administer a Meridian 1 system and its subsystems.

The STA application can co-reside with other MSDL applications to ensure flexible utilization of MSDL port resources. Please refer to *System Management Applications* (553-3001-301) for more information.

Set-Based Administration

Set-Based Administration simplifies system installation and administration by enabling a set to be used to perform several administrative and maintenance procedures. Set-Based Administration is available for all system types, including additional feature enhancements. Please refer to *Set-Based Administration* (553-3001-303) for more information.

Meridian 1 and Succession Communication Server for Enterprise 1000

System Management

Information is subject to change without notice.Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at this own expense.
SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.
Publication number: 553-3001-300
Document release: Standard 6.00
Date: January 2002
Printed in Canada

NORTEL NETWORKS™