Meridian 1

X11 System management applications

Document Number: 553-3001-301
Document Release: Standard 8.00
Date: April 2000

Copyright ©1995–2000 Nortel Networks
All Rights Reserved

Printed in Canada

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 their own expense.

SL-1 and Meridian 1 are trademarks of Nortel Networks.

Revision history

April 2000

Standard 8.00. This is a global document and is up-issued for X11 Release 25.0x.

November 1999

Standard 7.00. Reissued to update technical content.

August 1996

Standard 6.00 for X11 Release 22.0x.

December 1995

Standard 5.00.

July 1995

Standard 4.00. This document is issued to indicate X11 Release 21.0x changes.

December 1994

Standard 3.00. Reissued to include editorial changes and indexing.

October 1993

Standard 2.00. This document includes updates and changes, as well as information for Voice Mailbox Administration.

August 1993

Standard 1.00.

Contents

Introduction

Reference List

- *X11 Administration (553-3001-311)*

This document describes the Meridian 1 system management applications. The applications are described in modules *arranged alphabetically by application name*. Each application module contains the following information:

— Status box

— Overview

— Operating parameters

— Interactions

— Packaging

— Implementation

— Operation

Status box

In the upper right-hand corner of the module's first page, the status box identifies the X11 Release when this application was first available, as well as the latest issue date of the application module.

Overview

Immediately following the title, the overview describes this application and any enhancement made to the original design.

When there is an enhancement, note the required X11 Release identified in the descriptive text, as it can differ from the X11 Release of the original application.

Operating parameters

These details explain the hardware and software items required or prohibited for operating this application.

Feature interactions

An interaction description explains how this application is affected by, or affects, other applications and features.

Feature packaging

A brief list provides the package information (name, number, and mnemonic) for this application, as well as its dependencies.

Feature implementation

This shows the individual overlays (LDs) necessary to activate this application. The overlays listed show only the prompts requiring responses for this application. For a complete discussion of prompts and responses, refer to the *X11 Administration (553-3001-311)*.

Feature operation

Follow these procedures to learn how to use this application.

History File

The Meridian 1 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.

History File

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, such as those for a disk/tape unit enable/disable
- TTY logins and logouts (with X11 Release 19 and later)
- Regular hourly time stamps (with X11 Release 19 and later)
- 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

You can specify one history file 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, with X11 Release 19 and later, 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 relating to service changes, traffic (if not redirected to a Traffic Log File), CDR activity, software bugs, and so forth. Messages recorded in a TTY Log File are not written to the History File.

Traffic Log File

With X11 Release 19 and later, you can specify one Traffic Log File 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 (VHST)

With X11 Release 19 and later, 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 Table 1 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 (added with X11 Release 19) facilitate identifying and locating relevant messages in a large file.

Operating parameters

You must 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 you request a printout.

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 reinitialized after a system reload.

Feature packaging

History File (HIST), package 55, has no feature package dependencies. X11 Release 19 and later adds the Traffic Log File and VHST capabilities to the History File package.

Feature implementation

LD 17 – Implement the History File feature prior to X11 Release 18.

Prompt	**Response**	**Description**
REQ	CHG	Change.
TYPE	CFN	Configuration data block.
IOTB	(NO) YES	Change input/output terminals or devices.
HIST	0–65534	History File size in characters.
ADAN	NEW HST	Create the History File.
	CHG HST	Change the History File.
USER	MTC, SCH, TRF, BUG, CSC	Message types to be stored in the History File.

LD 17 – Implement the History File feature with Release 18 and later.

Prompt	Response	Comment
REQ	CHG	Change.
TYPE	CFN	Configuration Record.
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, with X11 Release 19 and later).
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 you plan to implement a Traffic Log File, then make the History File the only device with a USER of TRF. If you give a USER of TRF to a TTY Log File, the Traffic Log File may contain extraneous TTY messages.

LD 17 – Implement the Traffic Log File (X11 Release 19 and later).

Prompt	Response	Comment
REQ	CHG	Change.
TYPE	CFN	Configuration Record.
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, with X11 Release 19 and later).

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

Prompt	**Response**	**Comment**
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 (with X11 Release 19 and later) to view either the History or Traffic Log File.
_VHST	xxxx, **	VHST command; ** to exit VHST mode.

Feature operation

X11 Release 19 introduces the View History File command. A response of 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 Table 1.

Table 1
VHST commands in LD 22 (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.
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.

Table 1
VHST commands in LD 22 (Part 2 of 2)

Prompt	Response	Description
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

— User logout message format:

TTY #nn LOGGED OUT <User Name> hh:mm dd/mm/yyyy
SESSION DURATION hh:mm

Example:

TTY #00 LOGGED OUT ADAMS 13:25 05/28/93
SESSION DURATION 00:07

Limited Access to Overlays

Reference list

The following are the references in this section:

- *X11 Administration (553-3001-311)*

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

— access to specific overlays

— modification of specified customer data

— access to specific tenant numbers

— access to Speed Call lists via the print routines in Overlay 20

— access to the configuration record (CFN) in Overlay 17:

- no access at all
- changing a user’s own password only
- full access to configuration information

- access via 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 Overlay 02 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 *X11 Administration (553-3001-311)*.

Beginning with X11 Release 19, 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 Overlay 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 2, which the system administrator can change using Overlay 17.

Table 2
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 nonunique 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 you must use it to access Overlay 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
- CRAFTSPERSON

Via Overlay 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 via 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. As of X11 Release 19 and later, 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 3
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 Overlay 17 and that is already up and running. If LNAME_OPTION in Overlay 17 is set to YES, the system assigns unique login names for all passwords, including PWD1 and PWD2. (See Table 2 on page 22.) With LNAME_OPTION left at NO (the system default), all passwords must be unique. Use Overlay 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 23.)

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 (X11 Release 19 and later), 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

This feature has no interactions with other feature packages.

Feature packaging

Limited Access to Overlays (LAPW) is available as package 164, which must be enabled for this feature to operate.

Feature implementation

Implementing the LAPW feature requires you to change the Configuration Record (CFN), LD 17. You must respond to the following prompts in LD 17:

LD 17 – Define LAPW options and passwords (Part 1 of 2)

Prompt	Response	Comment
REQ	CHG, END	Change data or terminate overlay.
TYPE	CFN	Configuration data block
PWD	YES	Prompt / response
PWD	YES	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_NA ME	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_NA ME	dd...d	Login name for Level 2 password; up to 11 characters chosen from 0–9 and A–Z
LAPW	nn	LAPW password number to change (0–99)
	X nn	X nn removes password nn.
	<cr>	End changes to LAPW passwords.
PWnn	dd...d	New password for LAPW password number nn; 4–16 characters chosen from 0–9, A–Z, and a–z
	<cr>	No changes to password nn
LOGIN_NA ME	dd...d	Login name for password nn; up to 11 characters chosen from 0–9 and A–Z

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

Prompt	**Response**	**Comment**
- 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, ALL	(No customers), customer number, or all customers
- TEN	xxx xxx...xxx, ALL, (XALL)	Tenant list for the above customer for password access. XALL removes tenant access for this password.
HOST	(NO) YES	Host mode
- OPT		Password Options
	(CFPA) CFPD	Changes to all LD 17 prompts (Allowed) Denied
	(LLCD) LLCA	Line Load Control commands (Denied) Allowed
	(FORCD) FORCA	(Deny) Allow user to invoke the FORCe command (requires that Multi-User Login be equipped)
	(MOND) MONA	(Deny) Allow user to invoke the MONitor command (requires that Multi-User Login be equipped)
	(PROD) PROA	Print Only Class of Service (Denied) Allowed
	(PSCA) PSCD	Printing Speed Call lists (Allowed) Denied
LAPW	<cr>	Stop defining passwords.
- FLTH	0–(3)–7	Failed logon attempt threshold
- LOCK	0–(60)–270	Lockout time in minutes
- AUDT	(NO) YES	Audit Trail (denied) allowed
- -SIZE		Word size stored in the Audit Trail buffer
	(50)–1000	For Release 18 and earlier
	(50)–1500	For Release 19 and later
-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	Comment
REQ	CHG	Change password options
PWD2	<cr>	Level 2 master password
- LPWD	aaaa	Login Password for LAPW user
- NLPW	xx...x	New login password for LAPW user

LD 22 – Check options available for LAPW passwords (administrator)

Prompt	Response	Comment
REQ	PWD	Lookup password options
PWD2	xxxx	Level 2 master password

Note: LAPW password options are output to the active TTY only. Option format is shown below:

```
FLTH       x Failed logon attempt threshold
LOCK       xx Lock-out time in minutes
AUDT       aaaAudit 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   xxxCustomer number and tenant numbers accessible
HOST No Host mode
OPT        aaaa...Password options allowed
```

LD 22 – Print options for LAPW password (user)

Prompt	Response	Comment
REQ	PWD	Print passwords
PWD2	<cr>	Administrator’s password

Note: Options available to the logged on password are printed. The format is shown below:

```
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   xxxCustomer number and tenant numbers accessible
Host     NoHost mode
OPT      aaaa... Password options allowed
```

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 27.

Meridian 1 Fault Management

Meridian 1 Fault Management helps simplify the task of maintaining a Meridian 1 system and its Application Processors. The X11 Release 19 enhancements described here assist the craftsperson in timely and accurate problem determination and resolution.

Note that there is new Fault Management capability in X11 Release 22 software. Refer to the next chapter on page 45 for more information.

Alarm filtering

An *alarm* is an X11 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 Meridian 1 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 Meridian 1 alarms will be incorrect.

Feature interactions

None.

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 Exception Filter data (Part 1 of 2)

Prompt	**Response**	**Comment**
REQ	CHG	Change existing information
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>	Create a new Alarm Filter entry Change an existing entry Remove an existing entry Remove an existing entry Exit Alarm Filter entry
TRIGGER	aa...aa	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
	<cr>	Retain the current value for this parameter.
SEVERITY		Identify the severity of the alarm type to be filtered:
	Critical MAjor MInor (None) <cr>	Conditions that threaten operational status Serious but operational conditions Other error conditions Conditions with no severity rating Retain the current value for this parameter

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

Prompt	Response	Comment
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 OUT X <cr>	Create a new Exception entry Remove an existing entry Remove an existing entry 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 4.

Table 4
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 Options: 81/61C/51C

— Severity Level:

The four severity levels, from least to most severe, are None, Minor, Major, and Critical. See SEVERITY in “LD 17 – Configure Alarm and Exception Filter data” on page 35, 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 “LD 17 – Configure Alarm and Exception Filter data” on page 35.)

— 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 Meridian 1 system.

Exception Filter List

The Exception Filter List is simply a list of specific alarm triggers, which are defined on page 36.

TTY output device

In X11 Release 19 and later, when a terminal is assigned with a USER type of FIL in Overlay 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 for how to configure the terminal.

LD 17 – Defining a terminal to receive filtered alarms

Prompt	Response	Comment
REQ	CHG	
TYPE	CFN	Change the configuration record
IOTB	Yes	Change the I/O devices table

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 Overlay 22.

LD 22 – Printing the Alarm Filter List and Exception List

Prompt	Response	Comment
REQ	PRT	
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 Overlay 2.

LD 02 – Printing 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
```

System Message Lookup Utility

The System Message Lookup Utility is available exclusively to C processor (11C, 51C, 61C, 81, and 81C) systems. This utility provides the ability to perform online lookups of Meridian 1 alarm messages. The utility accepts Meridian 1 alarm mnemonics and provides a descriptive explanation of the event. It supports Look Up Last Error and Look Up Any System Message. See “Feature operation” on page 43 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

None.

Feature packaging

System Message Lookup Utility (SYS_MSG_LKUP) is available as (package 245) exclusively for option 81 systems.

Feature implementation

Not applicable.

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.

New Fault Management for X11 Release 22

For X11 Release 22, new Overlay 117 allows the administrator to:

1. configure the Release 22 Alarm Management feature
2. identify all Meridian 1 alarms
3. configure IP network interface addresses
4. perform all IP network related maintenance and diagnostic functions

Both Administration and Maintenance commands appear in LD 117.

New Command Format

LD 117 uses a new 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 you enter “?” in the COMMAND position, Help text will appear which presents all applicable command options. If you enter “?” in the OBJECT position, HELP text will appear which presents all applicable OBJECT options.

2 **Abbreviated Inputs** - The new input parser will recognize 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 Release 22 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.

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.

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.

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

Sample Event Preference Table (EPT)

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 48 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.

TTY Output Format of Events

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>

Field	Description
<severity>	"***" (critical); "**" (major); "*" (minor); " " (blank for info)
<report id>	The report id consists of an event category (e.g. BUG, ERR, etc.) and an event number (1200, 230, etc.). 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)
<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 SL-1 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 Meridian 1 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 M1 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 M1 system, two IP addresses must be specified: Primary and Secondary. A dual CPU M1 system operating normally will use the Primary IP address. A dual CPU M1 system operating in split mode (the mode used only when upgrading software or hardware) will use the Secondary IP address.

Remote Access

Remote access to Meridian 1 switches is made possible with Point-to-Point Protocol (PPP). LD 117 may be used to configure IP addresses for Point-to-Point Protocol.

LD 117 Command Descriptions

Command	Definition	Description
****	Abort	Abort overlay
BROWSE	Browse	Browse an existing System Event List
CHG	Change	Change/modify object configuration
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 Object Descriptions

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
FMT_OUTPUT	Formatted Output: Determine if system events uses formatted (also called fancy) or unformatted output. See "TTY Output Format of Events" on page 49 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 48 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 the table below, COMMANDS and OBJECTS are in bold typeface and fields are in regular typeface. Fields enclosed in brackets ( ) are default values.

=> **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 Meridian 1 active Ethernet interface IP address
CHG ELNK INACTIVE hostname	Set Meridian 1 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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **CHG SUPPRESS** entry.

=> **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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **CHG SUPPRESS** entry.
CHG FMT_OUTPUT OFF	Turn off formatted output
CHG FMT_OUTPUT ON	Turn on formatted output
CHG MASK nnn.nnn.nnn.nnn	Change subnet mask
CHG PPP LOCAL hostname	Set Meridian 1 local Point-to-point Protocol interface IP address
CHG PPP REMOTE hostname	Set Meridian 1 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)

=> **Command**	**Description**
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 48 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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **CHG SUPPRESS** entry.
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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **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 (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your **CHG SUPPRESS** entry.

=> **Command**	**Description**
NEW HOST hostname IPaddress	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 networkIP gateway IP	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 (e.g. 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
PRT EDT aa... a	Print a single Event Default Table (EDT) event, where: • aa... a = an event class with an event number (e.g. 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 (e.g. BUG1000, ERR0025) • bb...b = last entry in EDT event range (e.g. BUG1000, ERR0025)
PRT ELNK	Print active and inactive Ethernet interface IP addresses

=> **Command**	**Description**
PRT EPT aa... a	Print a single Event Preference Table (EPT) entry, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025
PRT EPT aa... a bb...b	Print specific Event Preference Table (EPT) entry, where: • aa... a = first entry in EPT event range (e.g. BUG1000, ERR0025) • bb...b = last entry in EPT event range (e.g. 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 entry(ies) information stored in database
PRT MASK	Print subnet mask stored in database
PRT OPEN_ALARM	Print open Simple Network Management Protocol (SNMP) traps setting
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 entry(ies) 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 48 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 (e.g. BUG1000, ERR0025)
RST ELNK ACTIVE	Reset Meridian 1 active Ethernet interface IP address to default value

=> **Command**	**Description**
RST ELNK INACTIVE	Reset Meridian 1 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
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.

=> **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
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

MSDL Serial Data Interface

With X11 Release 19 and later, 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 Meridian 1 and the MSDL.

The MSDL SDI supports three asynchronous serial data applications: TTY, PRT, and STA. (See “Single Terminal Access” on page 91.)

In addition to the data transmission parameters supported for an MSDL SDI port, you can specify a set of functions 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
- Overlay 2 and traffic measurements
- Filtered alarms
- Data administration

Functions

This section describes the major functions provided by the MSDL SDI in X11 Release 19 and later.

Autobauding

Autobauding is the ability of the MSDL to detect the baud rate of data transmission (from 300 to 38,400 bps) and report it to the Meridian 1. The Meridian 1 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 (LME)

Line mode editing permits the user to enter and review an entire line before transmitting it to the Meridian 1. 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 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 Meridian 1 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 Meridian 1.

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 reenabled.

However, if a craftsperson 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 reenabled.

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 5.

Table 5
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

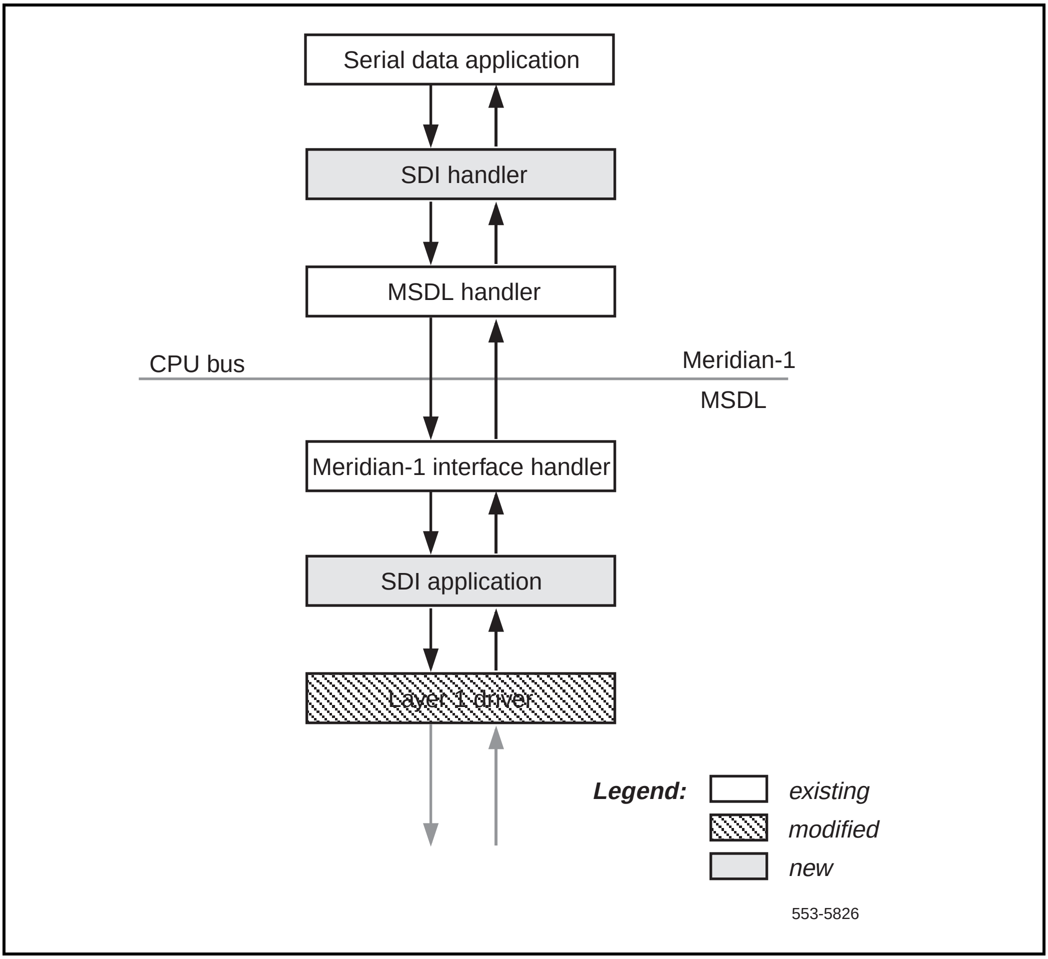
Note 2: User types of TRF, CTY, BGD

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 1 illustrates the software components that comprise the MSDL SDI, showing the different functional units.

Figure 1
MSDL SDI software components



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
- 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 that 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 reenabled manually through a maintenance overlay, or until it is reenabled 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 an option 81 in an SL-1 environment include the following:

- The SL-1 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.

In a PDT environment, the “s11pBegin” command is not supported for an option 81. 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 Meridian 1 assumes that the link is not responding.

Feature packaging

MSDL SDI is available as package 227. MSDL (package 222) is a prerequisite.

Feature implementation

The MSDL SDI is available for all machine types that support X11 Release 19 and later (except for option 11). It coexists on the MSDL with the CPSI, DCHI, MSPS, SDI, SDI2, SDI4, and XSDI cards.

There are a few 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 Overlay 17 activates the MSDL SDI.

LD 17 – Configuring MSDL SDI (Part 1 of 2)

Prompt	Response	Comment
REQ	CHG	Change
TYPE	CFN	Configuration record 1
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	0–4	Network group numbers (only prompted for option 81 phones)
DNUM	0–15	Device number; autoprinted by system in X11 Release 19 and later
PORT	0	Port number on MSDL card; autoprinted by system in X11 Release 19 and later if CTYP=MSDL
DES	aa...aa	Port designator; 1–16 characters, in the range of 0–9 and A–Z and some special characters (not including spaces, *, $, or #).
	Xaa	Precede entry with X to delete an existing name before trying to enter a new one.
BPS	300, 600, (1200), 2400, 4800, 9600, 19200, 38400	Baud rate
PRTY	(NONE), ODD, EVEN	Parity
STOP	(1), 1.5, 2	Stop bits
BITL	7, (8)	Data bit length
PARM	aaa bbb	Port functions. Where aaa = R232 or R422 and bbb = DTE or DCE. Default is: R232 DCE for TTY, R232 DTE for PRT.

LD 17 – Configuring MSDL SDI (Part 2 of 2)

Prompt	**Response**	**Comment**
FUNC		MSDL card function. Precede with an X to remove a function (for example, XLME)
	LME	Line mode editing
	ABD	Autobaud
	FCL	Flow control (XON/XOFF)
	SCN	Character screening
	MOD	Model support
USER		User types. When ADAN = HST, users may be BUG, MCT, MTC, or SCH or TRF.
	ACD	Automatic Call Distribution printer for reports
	APL	Auxiliary Processor Link for IVMS
	BGD	Background Terminal
	BUG	Software error
	CSC	Customer Service Changes
	CTY	CDR TTY port to output CDR records
	HSL	ACD/D High-Speed AUX link
	MTC	Maintenance
	NOO	No Overlay allowed
	PMS	Property Management System interface
	SCH	Service Change
	TRF	Traffic

Sample configurations

This section includes sample configurations for five situations:

1 An existing terminal to be used for regular maintenance functions

2 An MSDL SDI with a remote maintenance terminal

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

4 A printer port connected to a smart printer

5 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	Comment
REQ	CHG	Change
TYPE	CFN	Configuration
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	0–4	Network group number for option 81 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; X11 Release 19 and later supports only ENGLISH
DES	aaa...a	For example, Maint_TTY; up to 16-character designation; no blanks, *, $, or !
BPS	9600	Baud rate (default 4800)

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

Prompt	**Response**	**Comment**
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 your 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 you use 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) via modem

LD 17 – Prompts and responses for Sample 2

Prompt	Response	Comment
REQ	CHG	Change
TYPE	CFN	Configuration
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	0–4	Network group number for option 81 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; X11 Release 19 and later 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
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	Comment
REQ	CHG	Change
TYPE	CFN	Configuration
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	0–4	Network group number for option 81 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; X11 Release 19 and later supports only ENGLISH
DES	aaa...a	For example, Super_Terminal; up to 16-character designation; no blanks, *, $, or !

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

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

Prompt	Response	Comment
REQ	CHG	Change
TYPE	CFN	Configuration
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	0–4	Network group number for option 81 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; X11 Release 19 and later 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

Prompt	Response	Comment
REQ	CHG	Change
TYPE	CFN	Configuration
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	0–4	Network group number for option 81 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; X11 Release 19 and later 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 Meridian 1 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 Meridian 1 Interface Handler.

Port initialization occurs when the system software requests that an SDI port be enabled. The SDI application registers with the Meridian 1 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 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.

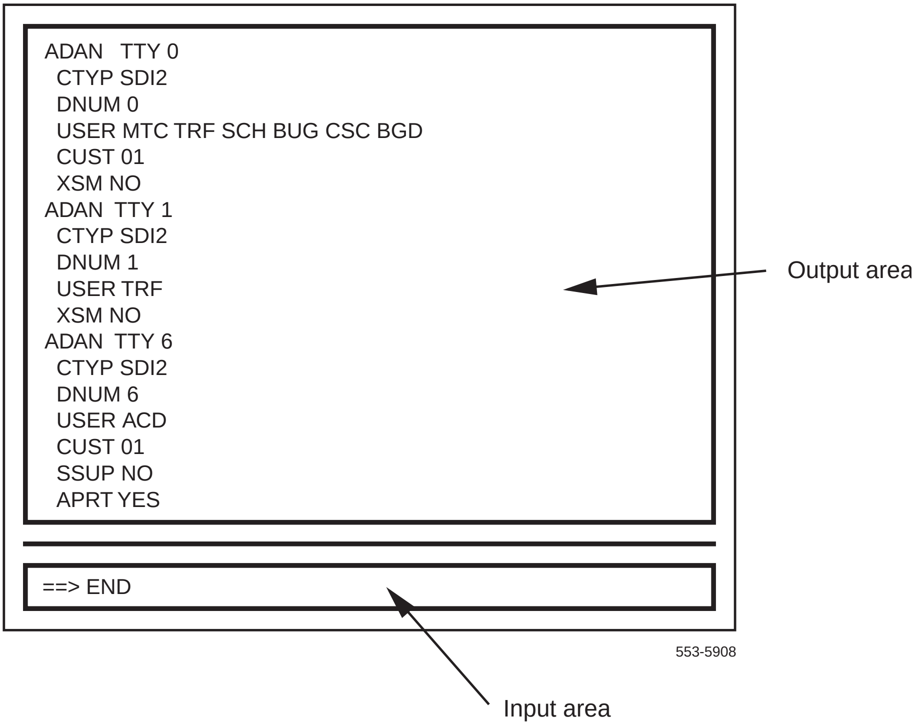
If an MSDL port has line mode editing turned on, the high order bit of an 8-bit character sent by the Meridian 1 is cleared, whether or not the Multi-Language TTY I/O package (211) is equipped.

XON/XOFF handling

Use this function if the SDI port is connected to a printer that cannot keep up with the Meridian 1 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.

Figure 2
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
```

```
==> END
```

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.

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 Meridian 1 Interface or Layer 1 Driver fails, the Meridian 1 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

Meridian 1 Multi-User Login (MULTI_USER) (package 242) enables up to three users to log in, load, and execute overlays simultaneously. These three users are in addition to an attendant console or maintenance terminal. The multi-user capability increases the efficiency of technicians by enabling them to perform tasks in parallel. To facilitate this operating environment, Multi-User Login includes significant functionality:

— 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 88 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 Overlay 17 creates a log file of the specified size for the TTY.

Overlay 22 supports viewing (printing) of a TTY log file. (See “Feature implementation” on page 86 for specific instructions.)

Changes for X11 Release 22 and later

With X11 Release 22 and later, the number of users allowed to log in at the same time is increased to five. Multi-User capability is also extended to LD 2 and LD 87.

Operating parameters

To use Multi-User Login on non-option 81 systems requires that the Overlay Cache Memory feature be active. With multiple concurrent sessions, overlays execute from the cache memory area.

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).

For three users to log in and use different overlays at the same time requires a minimum of four cache buffers; eight is recommended. Each buffer requires 19,000 words of memory.

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 6, on page 85.

Table 6
Sample overlay combinations supported in X11 Release 19 and later

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 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 21 for more information.

Feature packaging

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

Feature implementation

Use LD 17 to activate Multi-User Login.

LD 17 – Multi-User Login

Prompt	Response	Comment
REQ	CHG	Change
TYPE	OVLY	Overlay gateway
SID	<cr>	System ID number
CACHE	xx	Overlay cache memory areas; must be at least 4; not valid with option 81
PRTY	xx xx xx xx xx	Set priority for stored overlays (the recommended priority is 10 11 20 21 22); not valid with option 81
MULTI_USER	(OFF) ON	(Deactivate) Activate multi-user login

Also use LD 17 to allow or disallow the FORCe and MONitor commands.

LD 17 – Allow or disallow the FORC and MON commands

Prompt	Response	Comment
REQ	CHG	
TYPE	PWD	Configuration record
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

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

Feature operation

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

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

User commands

A user can issue the commands listed and described in Table 7, “New user commands,” on page 89 at the > prompt (after login but with no overlay executing), or from within an overlay. To issue a command from within an overlay, precede the command with an exclamation point (!).

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

```
!WHO
```

Table 7
New user commands

Command	**Description**
WHO	Displays 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	Sends 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	Sends 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	Prevents messages sent by other terminals from appearing at the user's terminal.
SEND ON	Enables messages sent by other terminals to appear at the user's terminal.
FORC xx	Forces terminal xx to log off (the requesting user must log in with LAPW or a level 2 password).
HALT	Stops background and midnight routines during a login session.
HALT OFF	Resumes halted background and midnight routines.
MON xx	Initiates 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	Turns off the monitor function.
SPRT xx	Assigns printer output to port xx.
SPRT OFF	Resets printer output assignment.

Single Terminal Access

Single Terminal Access (STA), available with X11 Release 19 and later, provides integrated access to Operations, Administration, and Management (OA&M) functions for the systems it monitors, thus reducing the number of physical devices needed to administer a Meridian 1 system and its subsystems.

The STA application can coreside with other MSDL applications to ensure flexible utilization of MSDL port resources.

Terminology

Single Terminal Access introduces several technical terms. Definitions are provided here for your 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 (in X11 Release 19 and later) 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 Meridian 1 and its attached subsystems that 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 craftsperson can perform integrated system access functions.

STA Terminals

Local or remote VT220s or equivalents that are connected to STA-equipped MSDLs.

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

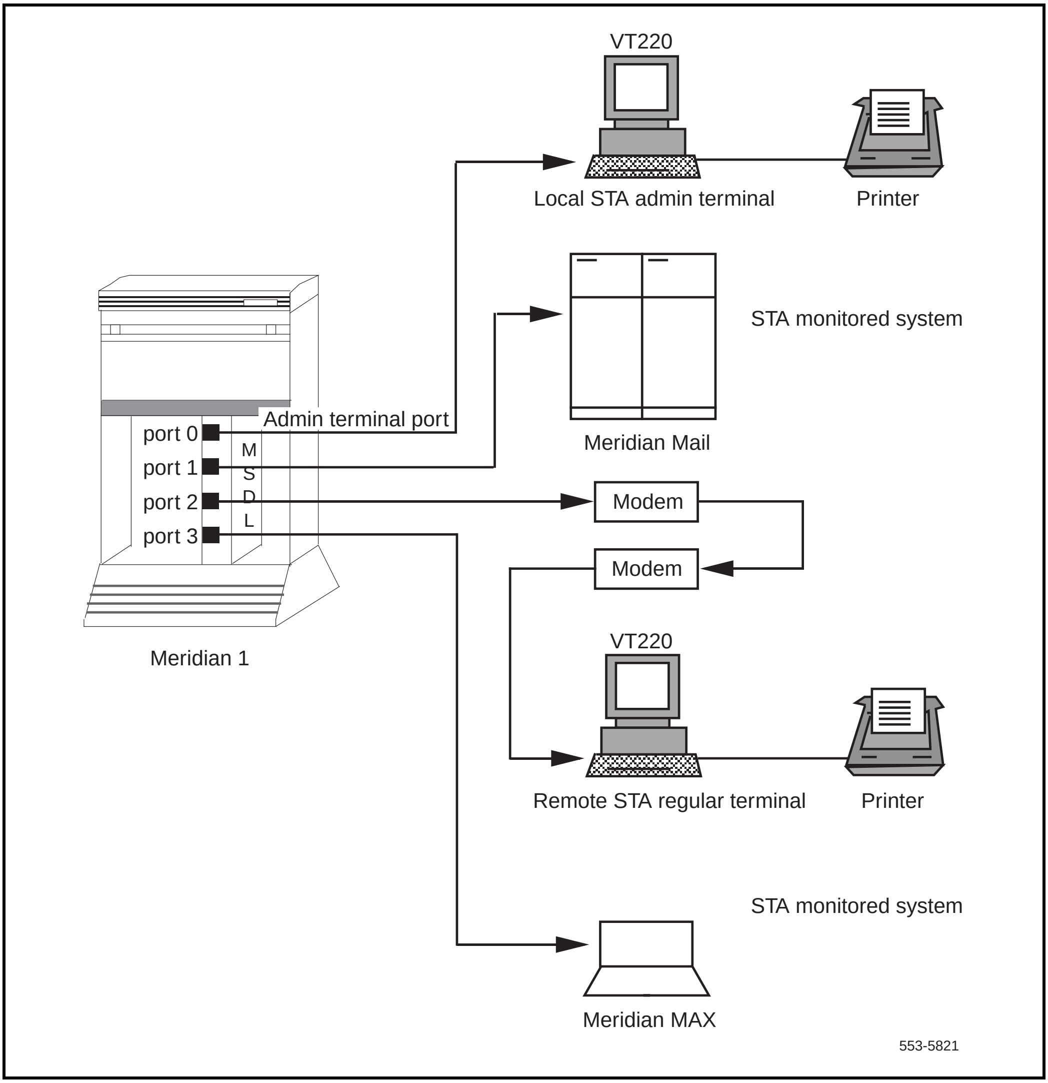
STA supports connections between ports with different baud rates. For example, an STA terminal at 9600 baud can connect to Meridian Mail at 2400 baud. In X11 Release 19 and later, STA supports up to 150 buffers of approximately 50 bytes each for data rate adaptation.

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 62 of the MSDL SDI module.

— MSDL port sharing

MSDL ports (except for the MSDL SDI) that are not used by STA are available for configuring other MSDL applications.

Figure 3
An STA-Monitored System with STA Administration and Regular Terminals



— Multiple connectivity

With multiple configured STA terminals, each can establish multiple, simultaneous connections to its monitored systems. For Meridian 1 access, STA uses the MSDL SDI interface. Subsystem access does not require Meridian 1 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 8.

Table 8
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

In X11 Release 19 and later, 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 (via 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 Meridian 1 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 9 for possible port assignments.

Table 9
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 in X11 Release 19 and later 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

In X11 Release 19 and later, 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.

In X11 Release 19 and later, the following machine types support STA: ST, XT, NT, RT, option 81. 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 Meridian 1 performs a sysload when STA is enabled, the SYSLOAD and INIT messages appear only on the terminal connected to the Meridian 1.

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

— Meridian 1 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 Meridian 1 system access.

Feature packaging

Single Terminal Access (STA), package 228, requires MSDL (package 222) and MSDL SDI (package 227).

Feature implementation

STA requires specific cabling and connections, as shown in Figure 4. 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.

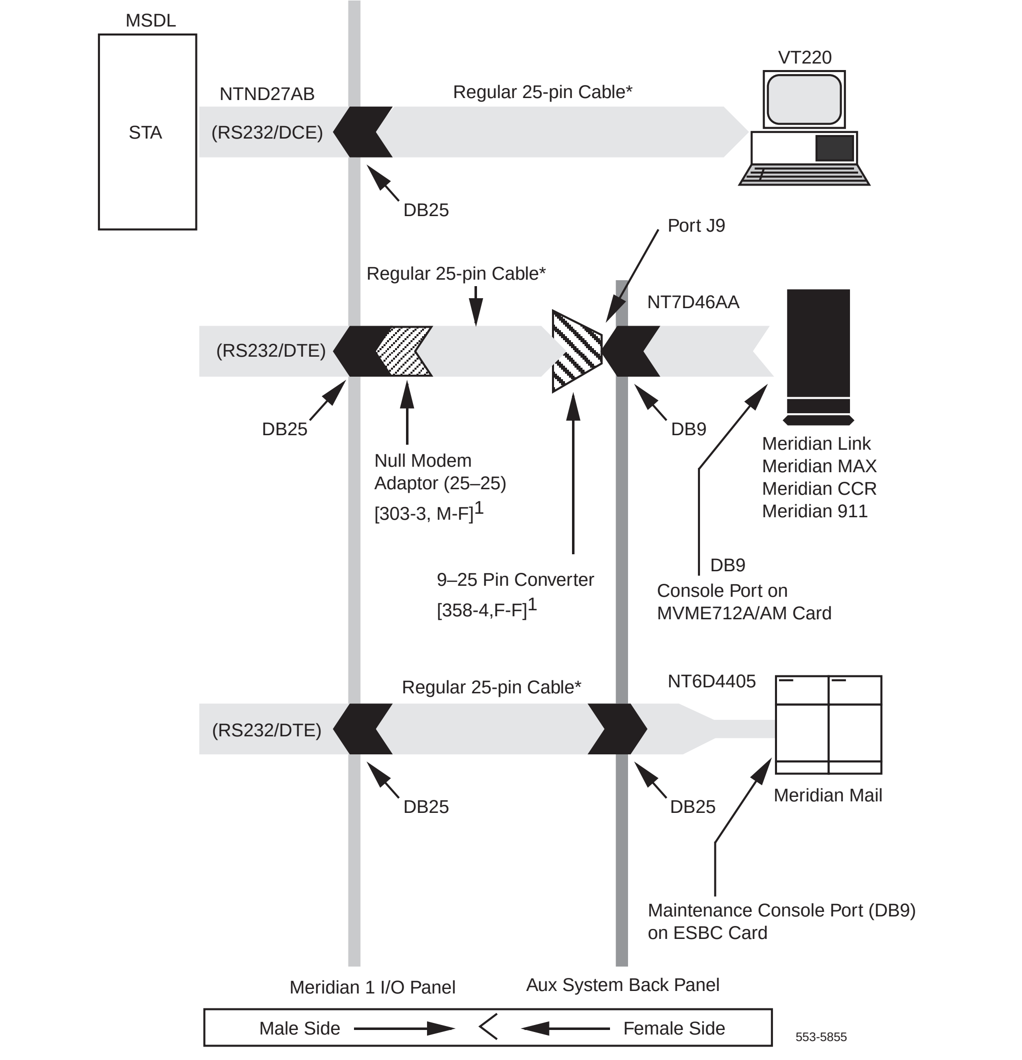
On page 116 of this module is an STA Planning Form to assist you in preparing for an STA implementation.

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 (222), MSDL SDI (227), and STA (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 61 for assistance.)

Figure 4
STA cable and connection information



*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 10 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 113 shows the setup for a VT420 terminal.

Table 10
Recommended setup for the STA terminal

General Parameters:	
Parameter	**Default STA Terminal Setup**
Terminal Mode	**EM200, 8-bit control**
On-line	Yes
Columns	80
Smooth Scroll	**No**
Cursor Off	No
Inhibit Auto Wrap	Yes
New Line	No
Multi Page	No
Interpret Control	Yes
User Features Lock	No
User Define Key Lock	No
Numeric Mode Keypad	Yes
Normal Mode Cursor Key	Yes
National Character Set	No
Frame Rate	72
Display Off After	15
Terminal ID	**VT220**

Table 10
Recommended setup for the STA terminal

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	CFN	Configuration
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	0–4	Network group number for option 81 systems
DNUM	0–15	Device number for I/O ports
ADMIN_PORT	0	STA admin terminal port # (must be 0)
LANGUAGE	ENGLISH	Language for STA; X11 Release 19 and later 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 106 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 116 of this module. Also, arrange the port configuration using the information in Table 11, “Recommended port configurations for STA-monitored systems,” on page 110.
- 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 106.)
- 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 Overlay 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.

Meridian 1 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 Overlay 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 Meridian 1 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 (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 Meridian 1 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 Meridian 1 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 Meridian 1, 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 Overlay 48 to disable the STA application.

2 Remove the STA application using LD 17.

To remove an MSDL port from STA:

1 Use Overlay 48 to disable the STA application.

2 Use Overlay 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 Overlays 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 Overlay 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

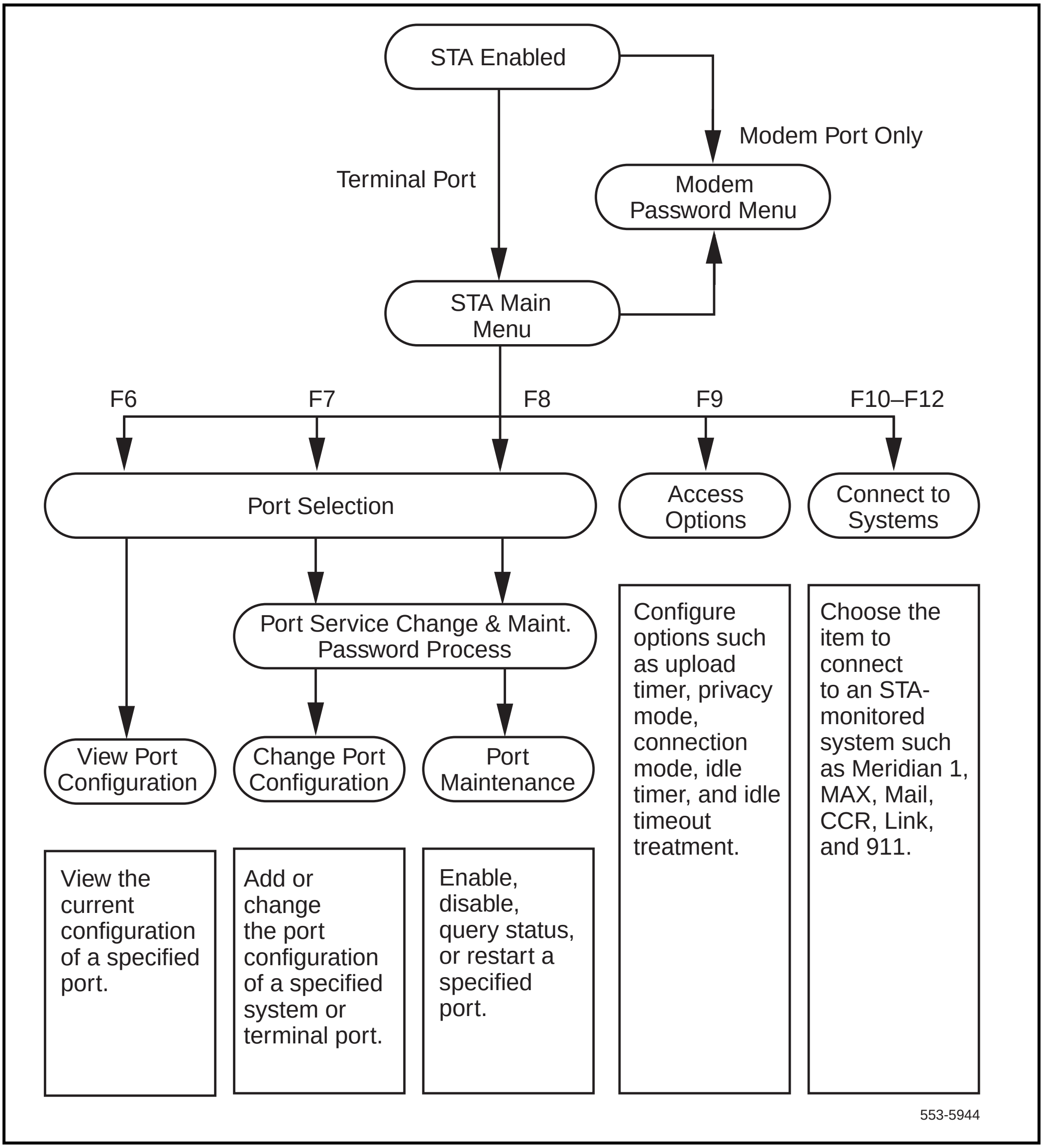
STA port commands

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

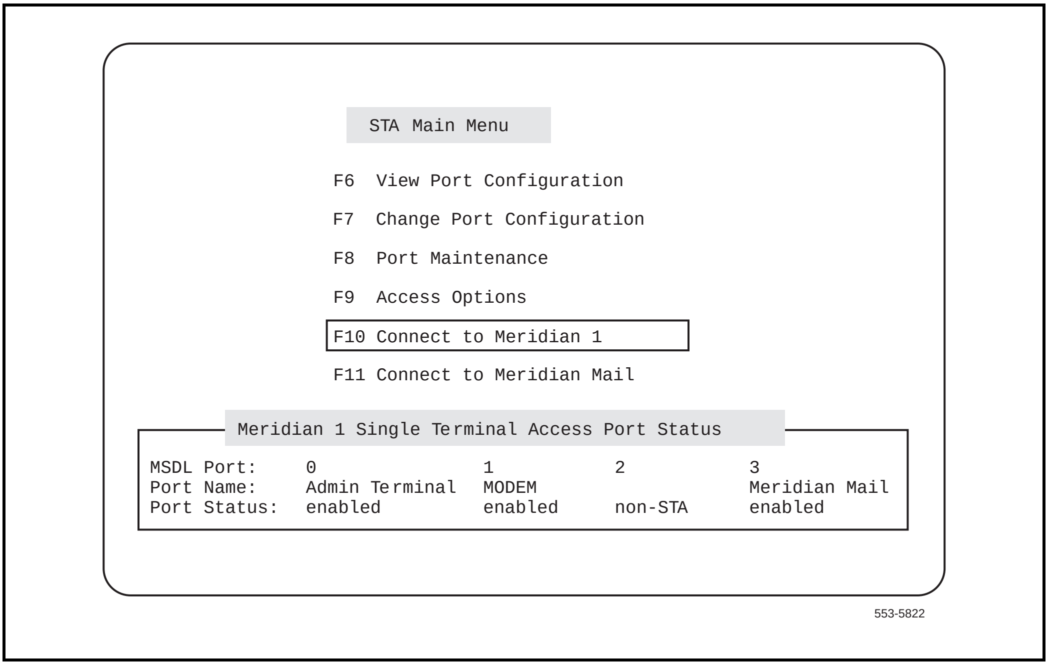
The user interface includes the STA Main Menu and several submenus. (Figure 5 shows the structure of the STA menus.)

Figure 5
STA menu structure


STA Enabled
Modem Port Only
Terminal Port
Modem Password Menu
STA Main Menu
F6
F7
F8
F9
F10–F12
Port Selection
Access Options
Connect to Systems
Port Service Change & Maint. Password Process
View Port Configuration
Change Port Configuration
Port Maintenance
Configure options such as upload timer, privacy mode, connection mode, idle timer, and idle timeout treatment.
Choose the item to connect to an STA-monitored system such as Meridian 1, MAX, Mail, CCR, Link, and 911.
View the current configuration of a specified port.
Add or change the port configuration of a specified system or terminal port.
Enable, disable, query status, or restart a specified port.
553-5944

To select an STA operation from the STA Main Menu, the user either presses the designated function key or moves the highlight bar to an operation and presses <CR>.

Figure 6
STA Main Menu



```
                    STA Main Menu

                  F6  View Port Configuration

                  F7  Change Port Configuration

                  F8  Port Maintenance

                  F9  Access Options

                  F10 Connect to Meridian 1

                  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
```

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.

> ***Note:*** If LAPW is equipped, the user name can be up to 11 characters and the password up to 16 characters. 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 11 lists the recommended port configurations for connecting to STA-monitored systems.

Table 11
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 Meridian 1 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 12.

Table 12
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	(Meridian 1), 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 Meridian 1

This operation causes the STA terminal to connect to the Meridian 1.

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 to enter a name (which may be optional)[1] and a required password. The password can be an SL-1 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.

[1] A name is required if LAPW is equipped and the login name option is on.

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[1]

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.

[1] PROCOMM PLUS is a registered trademark of DATASTORM TECHNOLOGIES, INC.

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

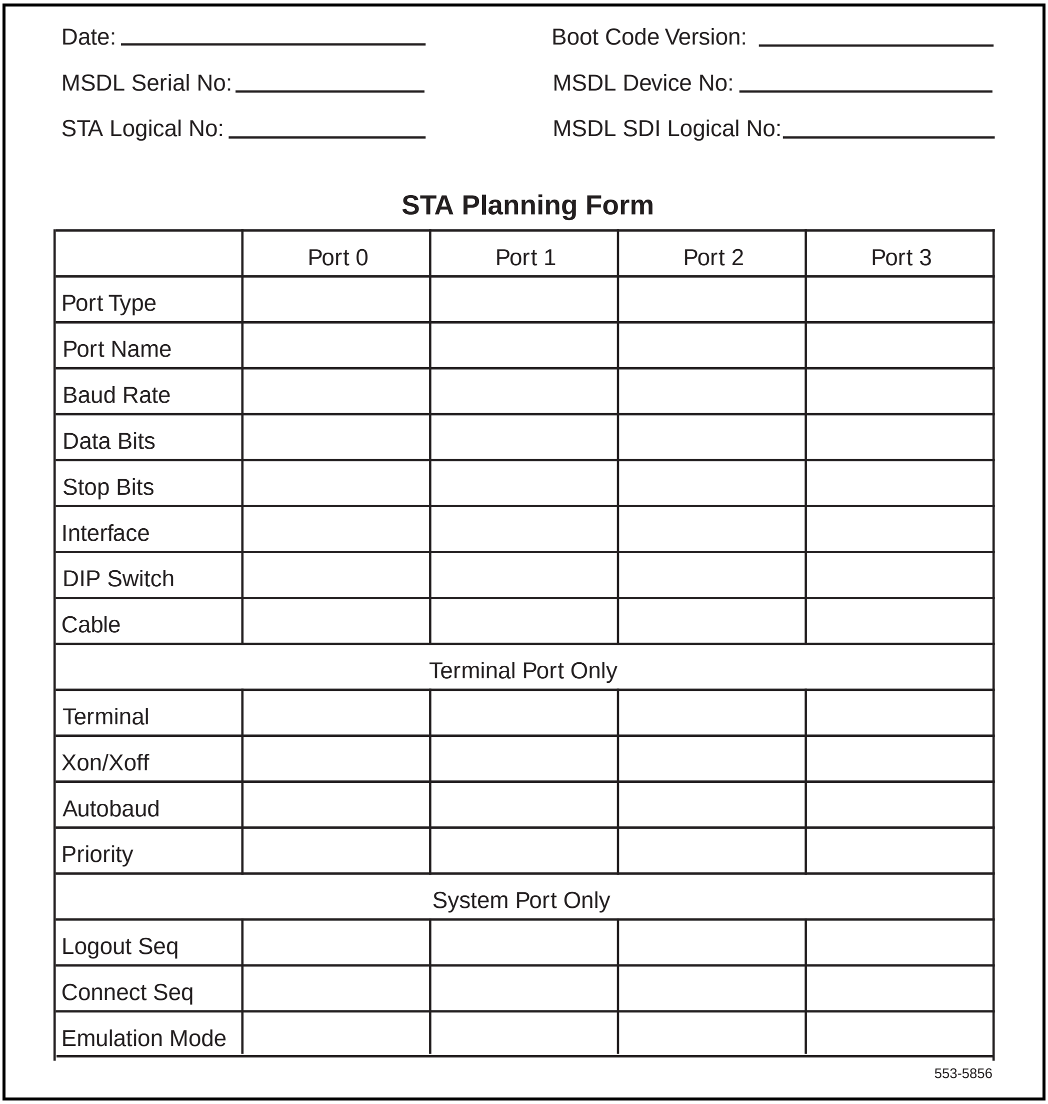
, < and . > Keys	< > Key	‘ ~ Key = Esc

Tab Setup screens

(Leave the defaults unchanged.)

STA planning form

Figure 7
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

Set-Based Administration

Reference list

The following are the references in this section:

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

Meridian 1 option 11 systems featured Set-Based Administration that simplified system installation and administration by enabling a set to be used to perform several administrative and maintenance procedures. Starting with X11 Release 21, Set-Based Administration is available for all system types, including feature enhancements.

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

— 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 (i.e., 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 of 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 option 11. 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 the option 11 the functionalities that have been offered by the Set-Based Administration prior to Release 21 are now grouped under the following two tasks on the main menu, under administration access:

- — Administration: provides a grouping 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 option 11, they will not be 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 SL-1 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 that 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.

Option 11 Set-Based Installation

The option 11 Set-Based Installation functions are not changed by the Set-Based Administration enhancements feature; however, the menu structure is altered.

Maintenance Sets

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

Prior to this development, the Set Relocation password was used for logging in through an Administration set. The Set-Based Administration enhancements feature decouples the Set Relocation password from the Set-Based Administration password.

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

Administration Set (ADMN) package 256 must be provisioned 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:

— Automatic Installation (AINS) package 200 (for the option 11 only)

— Calling PArty Name Display (CPND) package 95

— Digit Display (DDSP) package 88

— Meridian Modular Sets (ARIE) package 170

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 LDs 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

Prompt	Response	Comment
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[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[2]
- CUST	0-99	Customer number
- OPT		Specify permissions and restrictions associated with Set-Based Administration password PWNN. At least one permission must be given. The default is no permissions.
	(FEAD) FEAA	(Deny) allow Change Set Features (Administrator &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 (Option 11 Administrator & Installer access)

LD 17 – Define Set-Based Administration passwords

	(INSD) INSA	(Deny) allow.Installation Options (Option 11 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

Prompt	**Response**	**Comment**
REQ	NEW, CHG	Add or change
TYPE	FFC	Flexible Feature Codes (FFC) data block
CUST	0-99	Customer number
...		
CODE	ADMIN	Set-Based Administration - Administrator access FFC[1]
ADMIN	xxxx	Administrator access FFC
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 1: Only accepted if ADMINSET package equipped.		

LD 11 – Assign Maintenance Allowed Class

Prompt	Response	Comment
REQ	CHG	Change
TYPE	2008, 2016, 2216, 2616	
		BCS set with display option equipped
TN	lscu	Terminal number
	cu	Terminal Number for the option 11
...		
CLS	MTA	Maintenance allowed Class of Service

LD 17 – Define Login Types in History File

Prompt	Response	Comment
REQ	CHG	Change
TYPE	ADAN	I/O device data
ADAN	NEW/CHG/OUT HST	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[1]
Note 1: Only accepted if ADMINSET package is equipped.		

LD 17 – Increase the Maximum Number of Logins

Prompt	Response	Comment
REQ	CHG	Change
TYPE	PARM	Parameter data
...		

SBA_ADM_INS	0-(1)-2 (Opt 11E)
	0-(2)-64 (Opt 21-71)
	0-(2)-64 (Opt 81)
		Maximum Administrator and/or Installer logins allowed at one time (defaults in brackets)[1]

SBA_USER	0-(10)-20 (Opt 11E)
	0-(50)-250 (Opt 21-71)
	0-(100)-500 (Opt 81)
		Maximum User logins allowed at one time (defaults in brackets)[1]

Note 1: Only accepted if ADMINSET package is equipped.		

LD 17 – Increase Buffers

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

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 15 – Enable Use of Station Control Passwords

Prompt	Response	Comment
REQ	CHG	Change
TYPE	CDB	Customer Data Block
...		
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.[1]
PWD2	xxxx	If a response other than <cr> is entered for SBUP, the PWD2 password must be entered for confirmation.[2]

Note 1: Only prompted if the ADMINSET package is equipped and ACPL > 0.

Note 2: Only prompted if the response to SBUP is not <CR>.

LD 10, **LD 11** – Assign User Access Allowed Class of Service

Prompt	**Response**	**Comment**
REQ	CHG	Change
TYPE	xxxx	Type of set to be changed
TN	lscu	Terminal Number
	cu	Terminal Number for the option 11
...		
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**	**Comment**
REQ	NEW	Create new data
TYPE	ABCD	abcd key information
TBNO	1	Table number 1
PRED	YES	Data for predial keys
A	USER	Assign User FFC to key A

Meridian Mail Voice Mailbox Administration

Reference list

The following are the references in this section:

- *X11 features and services (553-3001-306)*

The Meridian Mail Voice Mailbox Administration (VMBA) feature enables the Meridian 1 system administrator to use Meridian 1 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 via LDs 10 and 11 rather than via a separate terminal
- viewing application and mailbox statistics to help ensure the integrity of the application

- synchronizing the Meridian 1 and Meridian Mail databases using special audit and upload functions
  - The audit function helps ensure that name data stored on the Meridian 1 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 Meridian 1 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 Meridian 1 for VMB administration when VMBA is equipped.

In X11 Release 19 and later, VMBA is supported on RT, XT, NT, and STE systems, as well as on options 21A, 21E, 51, 61, 71, and 81. Telephone types supported include the SL-1, Meridian Modular telephones, M2317, M2000, M3000, and 500/2500.

For a complete description of VMBA, refer to *X11 features and services (553-3001-306)*.

Index

Meridian 1

X11 System management applications

Copyright ©1995–2000 Nortel Networks
All Rights Reserved

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 their own expense.

SL-1 and Meridian 1 are trademarks of Nortel Networks.

Publication number: 553-3001-301
Document release: Standard 8.00
Date: April 2000
Printed in Canada

NORTEL NETWORKS

How the world shares ideas.