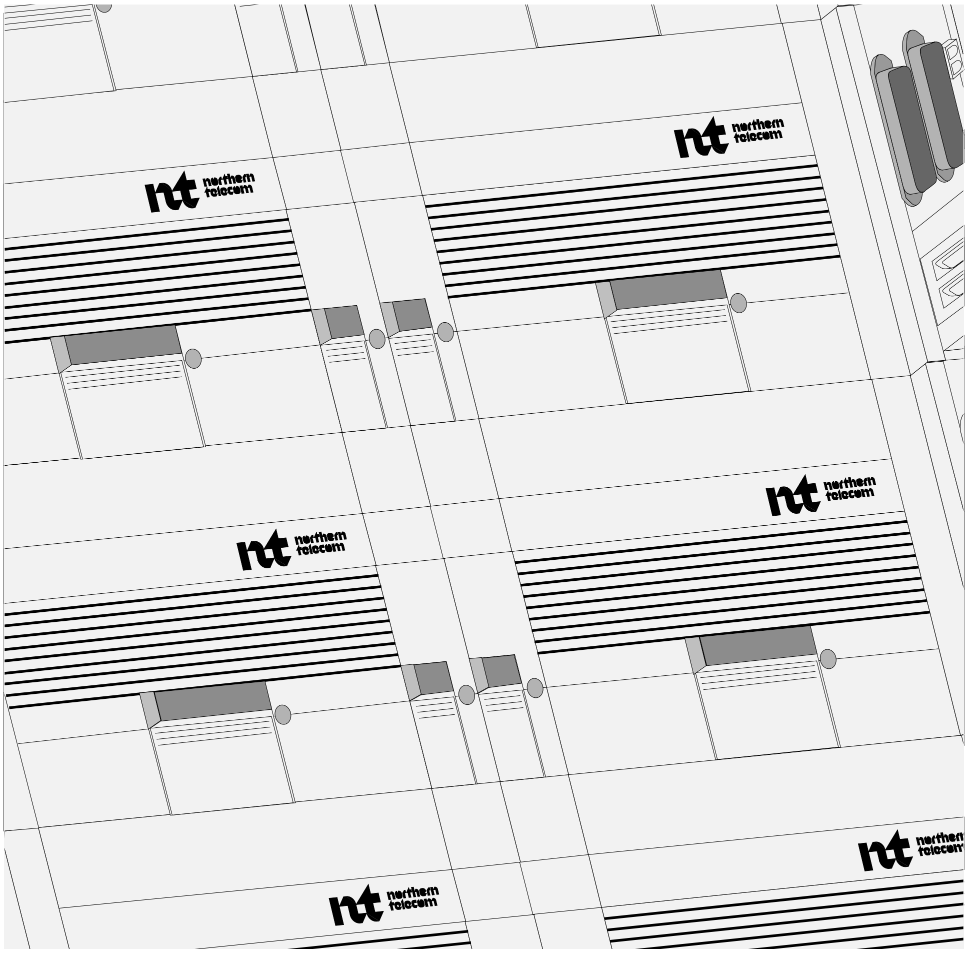
NT4K00LA **323-3001-840**

SONET Products

AccessNode

Log Report Manual

Issue 3.0 October 1999



NORTEL NETWORKS™

SONET Products

AccessNode

Log Report Manual

Document number: 323-3001-840
Document release: Issue 3.0
Date: October 1999

Printed in Canada

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

Publication history

October 1999

AN17.20 release of the document, Issue 3.0. Added information to the AIC tables regarding the LAIC “values” A, B, C, and D.

June 1999

Standard AN17 release of the document, Issue 2.0. Added references to the *UE9000 Voice OAM&P User Guide*.

February 1999

Standard AN16 release of the document, Issue 1.0. Changes include:

- NE ID range changed from 1-9999 to 1-32767
- maximum shelf numbers changed from 14 to 28
- added GEN605 and GEN750 log reports

June 1998

AN15 standard 01.01 release of the document. Changes include:

- ANX event chapter (Chapter 2) moved from this book to *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, in the *AccessNode Express* volume
- Changes to line card logs in LC section
- New VLCM log added

September 1997

AN14 standard 01.01 release of the document.

July 1996

AN12 standard 01.01 release of the document.

November 1995

AN11 standard 02.01 release of the document.

April 1995

AN10 standard release of the document.

December 1994

AN08 standard release of the document.

November 1994

AN07 reissue of standard.

April 1994

AN07 standard release of the document.

May 1993

FWP06 standard release of the document.

Contents

About this document

This document contains an explanation for each log report generated by AccessNode.

Log reports not listed in this document are generated by one of the following:

- base software and are documented in the *DMS-100 Log Report Manual*, 297-1001-840
- the AccessNode Express and are documented in the *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543

Audience

This document is for maintenance technicians and experienced users from Nortel Networks or a telephone operating company. This document applies to the current product release.

How to use this document

This document lists AccessNode log reports in alphabetical order. You can find your specific log simply by paging through the book.

References in this document

This document refers to the following documents:

Description, Volume 2A

- *Alarm and Surveillance Description*, 323-3001-104

Commissioning and Testing, Volume 3

Operations, Administration, and Provisioning, Volume 4B

- *Provisioning and Operations Procedures*, 323-3001-310

Maintenance, Volume 5A

- *Alarm and Trouble Clearing Procedures*, 323-3001-543

Maintenance, Volume 5C

- *Module Replacement Procedures*, 323-3001-547

AccessNode Express volume

- *AccessNode Express Alarm and Trouble Clearing Procedures,* 323-3051-543

DMS-100 SuperNode

- *DMS-100 Log Report Manual*, 297-1001-840

Subscriber Carrier Module (SMA)

- *Subscriber Carrier Module-100*, 297-8251-550

Overview of log reports

The AccessNode system informs the user of system occurrences through event reporting. An event is another name for a system occurrence. An example of an event is the initiation or termination of a process. When reporting an event, the system generates either an alarm, an alert, or a log.

> ***Note:*** For more information on events, see *Alarm and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A.

A log is an information-only notification that usually requires no action from the user. Logs record the incidence of an event as well as provide supplementary information to help fault location and troubleshooting. Logs are used to detect intermittent problems that are not severe enough to raise an alarm. Examples of events that logs report are:

- a change in operational state
- the completion or abnormal termination of a task
- an operational summary of the usage of a resource.

AccessNode refers to logs as “event log reports.” AccessNode event log reports are reported automatically to the user. An alphanumeric code, such as COM301 or NE402 identifies AccessNode event log reports.

Logs can be categorized as network element (NE) event logs and operations controller (OPC) event logs for AccessNode.

NE event logs

The NE event logs are divided into user logs and system logs. (System logs are used internally by software designers and are not intended for customer use.) The user log categories are:

- Communication (COML): events related to communication between NE-to-NE and NE-to-OPC.

- Equipment (EQP): events related to:
  - circuit packs
  - circuit pack groups
  - common equipment
  - shelf
  - frame hardware
- Event (EVNT): events related to internal routing of the following event reports:
  - alarms
  - logs
  - attribute changes
  - enrolls
- Facility (FAC): events related to facility provisioning (create, delete, state change, and parameter editing).
- Fault (FLT): event related to circuit pack alarms.
- Database (FWDB): events related to FiberWorld NE database operations, including:
  - database backup
  - database restore
  - journal entry
- Host Messaging Unit (HMU): events reported by the HMU processor on the Proc card, including:
  - errors detected by HMU software
  - HMU restart
  - HMU sanity time out
  - HMU software errors

  In the case of software errors (HMU901), Nortel Networks Technical Assistance should be contacted.
- Integrated remote test unit (IRTU): events related to the IRTU circuit pack.
- Line card (LC): events related to line cards and line terminations.
- Network Element (NE): events related to the creation, deletion, or modification to an NE.

- Optional (OPT): events related to the availability of optional features like parallel telemetry. An OPT log should be reported to NT Technical Assistance.
- Schedule (SCHD): raised when a scheduled event on the NE, such as database backups, exerciser options, and internal refresh/updates, could not be run. A single occurrence of this log does not necessarily indicate a problem, but repeated instances of a SCHD log should be reported to Nortel Networks Technical Assistance.
- Software (SOFT): indicates that the default mapper for the STS Bandwidth Manager is disabled.
- Software errors (SWERR and TRAP): events related to internal software operation. Because of their severity SWERR and TRAP logs are not documented in this NTP. Any SWERR or TRAP log occurrence should be reported to NT Technical Assistance.
- Test access card (TAC): events related to the test access circuit pack.
- Time division multiplexing (TDM) card: events related to the TDM. See the *UE9000 Voice OAM&P User Guide* for more information.
- Transaction processing system (TPS): events related to the transaction processing system. The TPS passes and receives messages from the Message Transport System (MTS).
- Universal Edge 9000 multi-circuit line card (UELC): events related to the UE9000 line circuits. See the *UE9000 Voice OAM&P User Guide* for more information.
- Virtual line concentration module (VLCM): events related to the lines on a VLCM, such as:
  - provisioning
  - deprovisioning
  - reprovisioning
  - line state change

OPC event logs

All OPC logs are considered user logs. Their categories include:

- Communication (COM): communication events between the NEs and the OPC.
- General (GEN): general OPC system-level events.
- Network administration and surveillance (NAD): events dealing with the installation and distribution of software loads to NEs, and the backup and restoration of the NE data.

- Software and data administration (SDA): events dealing with the installation and distribution of software loads to network element, and the backup and restoration of network element data
- Switch of activity (SWCT): events related to a switch of activity of the processor card on a network element.
- Standby (STBY): events concerning the status of the primary and backup OPCs.

Numbering scheme

The following numbering scheme indicates the nature of the event being logged.

300-399	Trouble	indicates a problem
400-499	Usage	indicates the use of a resource or service
500-599	State change	indicates a significant change in status
600-699	Completion	indicates that a process has been completed
700-799	Progress log	indicates that a process is underway

For details on the log reports fields, see Appendix A of this document.

Log report categories

Table 1-1 lists all the log categories documented in this book. Each category is listed on the left and the log page reference is on the right.

Table 1-1
Log report categories

Log category	See
AIC	page AIC-1
COM	page COM-1
COML	page COML-1
EQP	page EQP-1
EVNT	page EVNT-1
FAC	page FAC-1
FLT	page FLT-1
FWDB	page FWDB-1
GEN	page GEN-1
HMU	page HMU-1
IRTU	page IRTU-1
LC	page LC-1
NAD	page NAD-1
NE	page NE-1
OPT	page OPT-1
SCHD	page SCHD-1
SDA	page SDA-1
SOFT	page SOFT-1
STBY	page STBY-1
SWCT	page SWCT-1
TAC	page TAC-1
TPS	page TPS-1
VLCM	page VLCM-1

AIC300

Report explanation

This log is generated when the loopback access interface card (LAIC) software detects a maintenance event or a fault. If this log is generated, the LAIC has failed.

> ***Note:*** Faults are a result of a number of errors within a specific time interval. For example, if 5 section parity errors occur within 5 seconds, then a fault report is generated.

Report format

The following is the format for log report AIC300:

AIC300 <date> <time> <id number> <event_type> <event_label>
AIC <location> Resource: <class> Event: <event>

Report example

The following is a typical example of log report AIC300:

```
AIC300 MAY29 12:34:56 8800 TBL Fault
AIC B  Resource: CPU      Event: UNEXPECTED RESTART
```

—continued—

AIC300, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<date>	mmmdd	The date the log is generated
<time>	hh:mm:ss	The time the log is generated
<id number>	4 digit integer	The first two numbers are the global sequence of the log. The last two numbers are the device sequence number of the log.
<event_type>	Up to 4 characters: TBL	The log event type: TBL indicates that the log is reporting a system occurrence that is potentially service affecting.
<event_label>	Character string	Explains what the log is reporting, such as an LAIC `Fault`
<location>	A, B, C or D	Identifies the specific LAIC the log is reported against. **Note:** The LAIC "value" (A, B, C, or D) designates the following location in the ABM: AIC A is the LAIC in plane A, slot 13 AIC B is the LAIC in plane B, slot 16 AIC C is the LAIC in plane A, slot 12 AIC D is the LAIC in plane B, slot 15.
<class>	Text string: LCA MHIC1 MHIC2 CPU UNKNOWN	The component on the LAIC board that is detecting the fault: Loopback and Communication Access Multiport HDLC Interface Controller #1 Multiport HDLC Interface Controller #2 Central Processing Unit
—continued—		

—continued—

AIC300, continued

Field (continued)	Value (continued)	Description (continued)
<event>	Text string:	The specific fault detected:
		LCA events:
	LCA SANITY	LCA is not operating correctly
	LCA TFIFO1	transmit FIFO alignment error
	LCA TFIFO2	transmit FIFO alignment error
	LCA SECT PARITY	section parity error on LAIC
	LCA PATH PARITY	path parity error in receive path
	LCA FP ERROR	error in frame pulse from transport interface card (TIC)
		MHIC1 or MHIC2 events:
	B53-1 ERROR	fault in communications chip
	B53-2 ERROR	fault in communications chip
		CPU events:
	NO PING RESPONSE	firmware or CPU failure
		UNKNOWN events:
	UNEXPECTED RESTART	the firmware restarted unexpectedly
	HARDWARE ERROR	any other error

—end—

Action

Because the LAIC has failed, you need to return it to an in-service state. Diagnostics are run automatically when you return the LAIC to an in-service state.

For CPU errors, reload the LAIC firmware. If the CPU error continues, replace the LAIC circuit card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

For all other errors, if the LAIC continues to fail, replace the LAIC as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—end—

AIC301

Report explanation

This log is generated when a loopback access interface card (LAIC) restart fails.

Typically, if an LAIC restart problem occurs, this log is generated after an AIC720 log report.

Report format

The following is the format for log report AIC301:

AIC301 <date> <time> <id number> <event_type> <event_label>
AIC <location> Reason: Restart fail   Problem id: <problem id number>

Report example

The following is a typical example of log report AIC301:

```
AIC301 MAY29 12:34:56 1400 TBL Restart Fail
AIC A Reason:Restart Fail      Problem id:231
```

—continued—

AIC301, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<date>	mmmdd	The date the log is generated
<time>	hh:mm:ss	The time the log is generated
<id number>	4 digit integer	The first two numbers are the global sequence of the log. The last two numbers are the device sequence number of the log.
<event_type>	Up to 4 characters: TBL	The log event type: TBL indicates that the log is reporting a system occurrence that is potentially service affecting.
<event_label>	Character string	Explains what the log is reporting, such as an LAIC `Fault`.
<location>	A, B, C or D	Identifies the specific LAIC the log is reported against. **Note:** The LAIC “value” (A, B, C, or D) designates the following location in the ABM: AIC A is the LAIC in plane A, slot 13 AIC B is the LAIC in plane B, slot 16 AIC C is the LAIC in plane A, slot 12 AIC D is the LAIC in plane B, slot 15.
<problem id number>	Integer	Identifies the specific cause of the failure. (This information is useful only for Nortel Networks software developers.)

Action

Reload the LAIC. If the LAIC fails again, remove and reinsert the LAIC. If this also fails, replace the LAIC, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

—end—

AIC600

Report explanation

This log is generated when the LAIC restart completes successfully. This log should be generated after every AIC720 restart log if the restart is successful.

Report format

The following is the format for log report AIC600:

AIC600 <date> <time> <id number> <event_type> <event_label>
AIC <location> Restart complete

Report example

The following shows typical examples of log report AIC600:

```
AIC600 MAY12 12:34:56 8400 INFO Restart Success
AIC A  Restart complete
```

—continued—

AIC600, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	**Value**	**Description**
<date>	mmmdd	The date the log is generated
<time>	hh:mm:ss	The time the log is generated
<id number>	4 digit integer	The first two numbers are the global sequence of the log. The last two numbers are the device sequence number of the log.
<event_type>	Up to 4 characters: INFO	The log event type: INFO indicates that the log is reporting a system occurrence for user information only.
<event_label>	Character string	Explains what the log is reporting, such as an LAIC `Fault`.
<location>	A, B, C or D	Identifies the specific LAIC the log is reported against. **Note:** The LAIC “value” (A, B, C, or D) designates the following location in the ABM: AIC A is the LAIC in plane A, slot 13 AIC B is the LAIC in plane B, slot 16 AIC C is the LAIC in plane A, slot 12 AIC D is the LAIC in plane B, slot 15.

Action

No action is required.

—end—

AIC720

Report explanation

This log is generated when the loopback access interface card (LAIC) restarts.

The following three types of restart available for the LAIC are:

- “Reboot in progress” initializes the LAIC hardware, downloads the LAIC software from the OPC, and causes full LAIC on-board software initialization.
- “Cold reset in progress” causes full on-board LAIC software initialization with no software download.
- “Warm reset in progress” resets the LAIC metallic side relays with no on-board software initialization.

Report format

The following is the format for log report AIC720:

AIC720 <date> <time> <id number> <event_type> <event_label>
AIC <location> <restart type>

Report example

The following shows typical examples of log report AIC720:

```
AIC720 MAY12 12:34:56 8300 INFO Restart Attempt
AIC A Cold reset in progress
```

—continued—

AIC720, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<date>	mmmdd	The date the log is generated
<time>	hh:mm:ss	The time the log is generated
<id number>	4 digit integer	The first two numbers are the global sequence of the log. The last two numbers are the device sequence number of the log.
<event_type>	Up to 4 characters: INFO	The log event type: INFO indicates that the log is reporting a system occurrence for user information only.
<event_label>	Character string	Explains what the log is reporting, such as an LAIC `Fault`.
<location>	A, B, C or D	Identifies the specific LAIC the log is reported against. **Note:** The LAIC “value” (A, B, C, or D) designates the following location in the ABM: AIC A is the LAIC in plane A, slot 13 AIC B is the LAIC in plane B, slot 16 AIC C is the LAIC in plane A, slot 12 AIC D is the LAIC in plane B, slot 15.
<restart type>	Character string: Reboot in progress Cold reset in progress Warm reset in progress	Indicates the type of LAIC restart in progress

Action

No action is required.

—end—

AIC721

Report explanation

This log is generated when the loopback access interface card (LAIC) firmware reports an informational message. An informational message notifies the user that a system event has occurred, for example, a process is 50% complete.

Report format

The following is the format for log report AIC721:

AIC721 <date> <time> <id number> <event_type> <event_label>
AIC <location>: <event info>

Report example

The following are typical examples of log report AIC721:

```
AIC721 MAY29 12:34:56 7400 INFO Firmware Info
AIC B: (TextLog) tcslogci.aa14     (69)
TRACEBACK: 01037C04 0102489E 010246E0
           01024888 010246E0

AIC721 MAY29 12:34:56 7300 INFO Firmware Info
AIC A: (InfoLog) Dummy info log
```

—continued—

AIC721, continued

Field descriptions

The following table explains each of the fields in this log report.

<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>&lt;date&gt;</td><td>mmmdd</td><td>The date the log is generated</td></tr>
<tr><td>&lt;time&gt;</td><td>hh:mm:ss</td><td>The time the log is generated</td></tr>
<tr><td>&lt;id number&gt;</td><td>4 digit integer</td><td>The first two numbers are the global sequence number of the log. The last two numbers are the device sequence number of the log.</td></tr>
<tr><td>&lt;event_type&gt;</td><td>Up to 4 characters:
INFO</td><td>The log event type:
INFO indicates that the log is reporting a system occurrence for user information only.</td></tr>
<tr><td>&lt;event_label&gt;</td><td>Character string</td><td>Explains what the log is reporting, such as an LAIC Fault.</td></tr>
<tr><td>&lt;location&gt;</td><td>A, B, C or D</td><td>Identifies the specific LAIC the log is reported against.
<b>Note:</b> The LAIC “value” (A, B, C, or D) designates the following location in the ABM:
AIC A is the LAIC in plane A, slot 13
AIC B is the LAIC in plane B, slot 16
AIC C is the LAIC in plane A, slot 12
AIC D is the LAIC in plane B, slot 15.</td></tr>
<tr><td rowspan="2">&lt;event info&gt;</td><td>Character string</td><td>Identifies and gives information on the specific event that has occurred</td></tr>
<tr><td colspan="2"><b><i>Note 1:</i></b> (TextLog) Text Logs display TRACEBACK followed by a series of alphanumeric strings that give traceback information. Traceback information indicates where in the software code the log was generated. (This information is useful only to Nortel Networks software developers.)
<b><i>Note 2:</i></b> (InfoLog) InfoLogs display text strings that give information on the specific event that has occurred.</td></tr>
</table>

Action

No action is required.

—end—

AIC900

Report explanation

This log is generated to record a trap. The LAIC hardware detects a trap, which indicates that something has broken on the fundamental level of the LAIC hardware or software. A trap causes the LAIC to shut down. The access processing unit (APU) then attempts to restart the LAIC.

Report format

The following is the format for log report AIC900:

```
CM        AIC900 <date> <time> <id number> <event_type> <event_label>
    AIC <location>: Trap <x> of <n>: <trap text>
    SR: <statusreg> VO: <vector> FA: <illaddr>
    TB: <traceback>
```

Report example

The following is the format for log report AIC900:

```
CM       AIC900 JUN25 11:51:38 4000 TBL Firmware Trap
    AIC A: Trap 1 of 2: (ANELBLU.AA65) - 18:19:13.74
    SR:  2004 VO: C008 FA: FFFFFFFF
    TB:  010397B6 010263B2 010261F4 0102639C 010261F4

CM       AIC900 JUN25 18:43:08 3900 TBL Firmware Trap
    AIC A: Trap 2 of 2
    D0:  00000001 00090000 00000004 00000001
    D4:  00000027 00000000 00000000 00000000
    A0:  005FB81D 004D1629 004D1616 005FB804
    A4:  004D1616 005FB764 005FB714 005FB6F8
```

—continued—

AIC900, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<date>	mmmdd	The date the log is generated
<time>	hh:mm:ss	The time the log is generated
<id number>	4 digit integer	The first two numbers are the global sequence of the log. The last two numbers are the device sequence number of the log.
<event_type>	Up to 4 characters: TBL	The log event type: TBL indicates that the log is reporting a system occurrence that is potentially service affecting.
<event_label>	Character string	Explains what the log is reporting, such as an LAIC `Fault or Firmware trap`.
<location>	A, B, C or D	Identifies the specific LAIC the log is reported against. **Note:** The LAIC "value" (A, B, C, or D) designates the following location in the ABM: AIC A is the LAIC in plane A, slot 13 AIC B is the LAIC in plane B, slot 16 AIC C is the LAIC in plane A, slot 12 AIC D is the LAIC in plane B, slot 15.
<x> of <n>	Integer	x = the current entry of the log n = the total number of entries for this particular log
<trap text>	Alphanumeric string	Records additional information about the trap (This field is optional)
<statusreg>	16-bit integer in hexadecimal format	Records the contents of the central processor unit (CPU) status register when the trap occurred
<vector>	32-bit integer in decimal format	Records the vector number of the software code where the trap occurred
<illaddr>	32-bit integer in hexadecimal format	Records the illegal address that caused the bus or address task trap.
<traceback>	Set of 32-bit integers in hexadecimal format, normally terminated by `deaddead`	Records the software history (or path) that led to the trap
Note 1: The fields <statusreg>, <vector>, <illaddr>, and <traceback> report internal system messaging that is used only by Nortel Networks software developers.		

—continued—

AIC900, continued

Action

A trap is an extremely rare occurrence. If you get this log, forward it to Nortel Networks customer support for problem diagnosis and corrective action.

—end—

AIC901

Report explanation

This log is generated by the loopback access interface card (LAIC) application when a software error is detected. A software error is an unexpected software condition, such as an out-of-bound input argument passed to a function. A software error is not service affecting and the LAIC continues to operate correctly.

Report format

The following is the format for log report AIC901:

AIC901 <date> <time> <id number> <event_type><event_label>
AIC <location>: <sectionName> (<lineNumber>) data=<reason>
TRACEBACK: <traceback>

Report example

The following shows a typical example of log report AIC901:

```
AIC901 MAY12 12:34:56 7200 TBL Software Error
AIC A: tcslogci.aa14     (63) data=00000063
TRACEBACK: 01037BD8 0102489E 010246E0
           01024888 010246E0
```

—continued—

AIC901, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<date>	mmmdd	The date the log is generated
<time>	hh:mm:ss	The time the log is generated
<id number>	4 digit integer	The first two numbers are the global sequence of the log. The last two numbers are the device sequence number of the log.
<event_type>	Up to 4 characters: TBL	The log event type: TBL indicates that the log is reporting a system occurrence that is potentially service affecting.
<event_label>	Character string	Explains what the log is reporting, such as an LAIC `Fault`
<location>	A, B, C or D	Identifies the specific LAIC the log is reported against. **Note:** The LAIC “value” (A, B, C, or D) designates the following location in the ABM: AIC A is the LAIC in plane A, slot 13 AIC B is the LAIC in plane B, slot 16 AIC C is the LAIC in plane A, slot 12 AIC D is the LAIC in plane B, slot 15.
<sectionName>	Alphanumeric	Records the section of the software code where the error occurred
<lineNumber>	Numeric	Records the line number of the software code where the error occurred
<reason>	Integer	Records information on why the software error occurred
<traceback>	Set of 32-bit integers in hexadecimal format, normally terminated by `deaddead`	Records the software history (or path) that led to the software error
Note: The fields <sectionName>, <lineNumber>, <reason>, and <traceback> report internal system messaging that is used only by Nortel Networks software developers.		

—continued—

AIC901, continued

Action

Software errors are rare occurrences. If you get this log, forward it to Nortel Networks customer support for problem diagnosis and corrective action.

—end—

COM301

Report explanation

The communication log (COM) is generated when the connection to a client application is dropped while it is still logged into the background file transfer service (bftpd). The normal procedure requires the client application to log out of bftpd before bringing the bftpd connection down. This log might be caused by the sudden death of the client application, or most likely, by a communication problem between the OPC and the remote host on which the client application is running.

Report severity

Warning

Report format

The following is the format for a COM301 log report.

COM301 Lost connection to background file transfer service user <bftpd user ID> logged in from <bftpd client name>.

Report example

The following shows a typical example of a COM301 log report.

```
COM301 Lost connection to background file transfer service user
admin logged in from Network Manager netman03 (192.1.2.34).
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.

Action

Ask the system administrator of the OPC to verify the health of the underlying IP network.

—end—

COM310

Report explanation

This log is generated when the OPC fails to archive the logs from the network element.

Report severity

Warning

Report format

The following is the format for a COM310 log report.

COM310 Failed to archive logs from NE <ne name> <ne id>.

Report example

The following shows a typical example of a COM310 log report.

```
COM310 Failed to archive logs from NE <ne name> <ne id>.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne name>	Character string	Network element name
<ne id>	Decimal	Network element id

Action

Check that an association between the network element and OPC still exists, either through the network element user interface or OPC user interface.

—end—

COM400

Report explanation

This log is generated when a client application logs in to the background file transfer service (bftpd) on behalf of the specified user.

Report severity

Warning

Report format

The following is the format for a COM400 log report.

COM400 User <bftpd user ID> logged in to the background file transfer service from <bftpd client name>.

Report example

The following shows a typical example of a COM400 log report.

```
COM400 User admin logged in to the background file transfer
service from Network Manager netman03 (192.1.2.34).
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<bftpd user ID>	Character string	A valid OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager’s host name and IP address.

Action

None

—end—

COM401

Report explanation

This log is generated when a client application logs out of the background file transfer service (bftpd) on behalf of the specified user.

Report severity

Warning

Report format

The following is the format for a COM401 log report.

COM401 User <bftpd user ID> logged in to the background file transfer service from <bftpd client name>.

Report example

The following shows a typical example of a COM401 log report.

```
COM401 User admin logged in to the background file transfer
service from Network Manager netman03 (192.1.2.34).
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.

Action

None

—end—

COM501

Report explanation

This log report indicates that OAM&P data can flow normally from the network element to the OPC. It is commonly seen at the successful conclusion of a software download or manual reboot of a network element.

Report severity

Warning

Report format

The following is the format for a COM501 log report.

COM501 OPC to NE <equipment identifier> Sh <shelf identifier> link established.

Report example

The following shows a typical example of a COM501 log report.

```
COM501 OPC to NE 43 Sh 1 link established.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<equipment identifier>	Decimal number	Serial number of the network element
<shelf identifier>	Decimal number	Typical value is 1.

Action

None

—end—

COM502

Report explanation

This log report indicates that the communications link between the specified network element and the OPC has been lost.

Report severity

Major

Report format

The following is the format for a COM502 log report.

COM502 OPC to NE <equipment identifier> Sh <shelf identifier> link lost.

Report example

The following shows a typical example of a COM502 log report.

```
COM502 OPC to NE 43 Sh 1 link lost.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<equipment identifier>	Decimal number	Serial number of the network element
<shelf identifier>	Decimal number	Typical value is 1.

Action

If a software download is in progress, or if commissioning changes are being made on the network, such as deleting an NE, this is a normal response and no action is required. A COM501 log should follow to indicate that the process responsible for the interruption in communication has been completed and that communication has resumed.

If the COM501 log does not appear, this log may indicate a more serious situation, such as a cut in the fiber link resulting in the partitioning of the network.

—end—

COM505

Report explanation

This log report indicates that a network element cannot establish a communications link with the OPC. It appears when a network element tries to establish a link with the wrong OPC or when it tries to establish a link while it is already communicating with an OPC.

Report severity

Warning

Report format

The following is the format for a COM505 log report.

COM505 Link request from NE <equipment identifier> Sh <shelf identifier> not accepted; <reason>.

Report example

The following shows a typical example of a COM505 log report.

```
COM505 Link request from NE 43 Sh 1 not accepted; Link already
up.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<equipment identifier>	Decimal number	Serial number of the network element
<shelf identifier>	Decimal number	Typical value is 1.
<reason>	Unknown NE	The network element is unknown to the OPC.
	Link already up	A communications link has already been established between the network element and the OPC.

Action

If the reason field indicates Unknown NE, log in to the OPC as a SLAT user and verify that the primary and backup OPC addresses match those with which the network element is commissioned to communicate.

If the reason field indicates Link already up, no action is necessary. The network element will repeat its communication request at a later time.

—end—

COML301

Report explanation

This log is generated when the AccessNode receives a CMIS association message from a host provisioned as GR-303 MVI. Only proprietary IDTs should be sending CMIS association messages. This log indicates that there is a misconfiguration between the AccessNode and the DMS host. When this is the case, the DMS will not receive a response to its CMIS association messages, and thus will be unable to establish an association with the AccessNode.

Report format

The following is the format for log report COML301.

COML301 mmmdd hh:mm:ss nnnn event_type event_label
Host: <host number>
Host defined as GR-303 MVI and IDT defined as proprietary

Report example

The following shows a typical example of log report COML301.

```
COML301 MAR29 14:39:00 0400 TBL configuration mismatch
Host: 0
Host defined as GR-303 MVI and IDT defined as proprietary
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<host number>	range: 0 - 5	The number of this host, as provisioned from the OPC.

Action

Step	Action
1	On the OPC, check how the AccessNode’s links to this DMS are provisioned.
2	If the AccessNode’s links to this DMS are provisioned correctly, then change the VARTYPE field in table RDTINV for this RDT to the value “GENTMC”.
3	On the DMS, check the VARTYPE field for this RDT in table RDTINV.
4	If table RDTINV is correct, then re-provision the AccessNode’s links to this DMS as “GR-303 DMS” links.

—end—

COML601

Report explanation

This log is generated when CMIS association is set up from the calling application entity to the called application entity (AET). It will indicate this for local associations (such as NE UI) and remote associations (such as OPC information collection).

> ***Note:*** During a Subscriber Carrier Module-100 Access (SMA) switch of activity, the raising of this log is part of the AccessNode's normal operation. In this situation, the log should be disregarded.

Report format

The following is the format for log report COML601.

```
COML601 mmm:dd hh:mm:ss nnnn event_type event_label
      <atype> association set up from <idtype><id> to <idtype><id>
      Calling set: <net><sys><idtype><id><ap name><ae qual>
      Called set: <net><sys><idtype><id><ap name><ae qual>
```

Report example

The following shows a typical example of log report COML601.

```
COML601 APR01 01:09:40 0400 INFO CMIS assoc up.
     Local association set up from NE 1 to NE 1
     Calling aet:      1 1 NE    1 OAM   SrvrAe
     Called aet:       1 1 NE    1 OAM   SrvrAe
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<atype>		The type of association:
	Local	– association between two applications on the same NE (for example, UI and Object manager)
	Remote	– association between an application on this NE and an application on another node (for example, OPC UI to NE Object Manager)
<net>	Integer	Identifier for the network of the node
<sys>	Integer	identifier for the system of the node

—continued—

—continued—

COML601, continued

Field	Value	Description
<idtype>		The type of node:
	NE	Network Element
	OPC	Operations Controller
<id>	Integer	Identifier for the node id
<ap name>	character string: OAM	String identifying the application process: Operation, Administration and Maintenance
<ae qual>	Character string:	Identifying the application entity:
	CollectorAe	OPC
	SrvrAe	NE
	mngrAe	NE UI

—end—

Action

None

—end—

COML602

Report explanation

This log is generated when CMIS association is aborted.

> ***Note:*** During a Subscriber Carrier Module-100 Access (SMA) switch of activity, the raising of this log is part of the AccessNode's normal operation. In this situation, the log should be disregarded.

Report format

The following is the format for log report COML602.

```
COML602 mmm:dd hh:mm:ss nnnn event_type event_label
<atype> association from <idtype><id> to <idtype><id> aborted by <aborter>
   Calling aet: <net> <sys> <idtype> <id> <ap name> <ae qual>
   Called aet: <net> <sys> <idtype> <id> <ap name> <ae qual>
```

Report example

The following shows a typical example of log report COML602.

```
COML602 APR01 01:09:40 0400 INFO CMIS assoc down.
   Local association from NE 1 to NE 1 aborted by CMIS user
   Calling aet:  1 1 NE  1 OAM       SrvrAe
   Called aet:   1 1 NE  1 OAM       SrvrAe
```

—continued—

COML602, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<atype>		The type of association:
	Local	– association between two applications on the same NE (for example, UI and Object manager)
	Remote	– association between an application on this NE and an application on another node (for example, OPC UI to NE Object Manager)
<aborter>		The application that aborted the association:
	CMIS user	– aborted by the application that set up the association.
	CMIS provider	– aborted by the CMIS providing application due to a process death or flow controlled too long
	Pres. provider	– aborted by the presentation layer or by the initiator of a remote association.
<net>	Integer	Identifier for the network of the node
<sys>	Integer	Identifier for the system of the node
<idtype>		The type of the node:
	NE	Network Element
	OPC	Operations Controller
<id>	Integer	Identifier for the node id
<ap name>	Character string:	String identifying the application process:
	OAM	Operation, Administration and Maintenance
<ae qual>	Character string:	Identifying the application entity:
	CollectorAe	OPC
	SrvrAe	NE
	mngrAe	NE UI

Action

None

—end—

EQP317

Report explanation

A protection switch was denied or failed due to a problem with the protection card or the protection path over which the switch was to occur. A protection switch failure alarm is raised in conjunction with this log report.

Report format

The following is the format for log report EQP317.

```
EQP317 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: <class>
Operation: <operation>
Reason: <reason>
   NE: <ne>                    LOCATION: <location>
   EQP: <eqp>
   SHELF POS: <shelf p>        SHELF: <shelf>
   MEMBER: <member>
   SLOT: <slot number>         PEC: <product engineering code>
```

Report example

The following shows a typical example of log report EQP317.

```
EQP317 MAR26 14:17:24 2100 TBL Protection Activity
Object Class: Redundancy Group Member
Operation: Denied
Reason: Forced (Local)
   NE: 661                    LOCATION: 1
   EQP: 1 OC12 LTE
   SHELF POS: 1               SHELF: 1
   MEMBER: OC12 G1
   SLOT: 10                   PEC: NT7E02KC
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<class>	Text string identifying the object	Object that failed/denied the protection request
<operation>	Failed or Denied	The type of protection operation
	—continued—	

—continued—

EQP317, continued

Field	Value	Description
<reason>	Forced (Local) Manual (Local) Signal/Eqp Fail (Local) Signal Degrade (Local)	Protection Operation that failed or was denied Protection Operations
<ne>	integer	Network element number
<location>	integer	Data identifying the object instance which has its protection activity failed/denied.
<eqp>	alphanumeric	Equipment type
<shelf p>	integer	Shelf position
<shelf>	integer	Shelf number
<member>	alphanumeric	Circuit pack type and group number
<slot number>	integer	Slot number of the circuit pack in question
<product engineering code>	alphanumeric	Product engineering code for the circuit pack in question

—end—

Action

Check the alarm screen of the network element user interface for a protection switching alarm, then look up the alarm in *Alarm and Trouble Clearing Procedures,* 323-3001-543, in *Maintenance,* Volume 5A.

—end—

EQP322

Report explanation

This log provides the results of a failed manual diagnostic test for a circuit pack. If a manual diagnostic passes, it is reported in log report EQP609.

Report format

The following is the format for log report EQP322.

EQP322 mmm:dd hh:mm:ss nnnn event_type event_label
Location fields. See Appendix A.

```
TC FAIL:          <reason>
                  <reason>
```

Report example

The following are typical examples of log report EQP322.

```
EQP322 MAR26 14:17:24 2100 TBL Diag Fail
     NE: 1             LOCATION: 1
     EQP: 1 ABM RFT
     SHELF POS: 1      SHELF: CE
     CPG: TIC B
     SLOT: 14          PEC: <product engineering code>
TC FAIL:               Access and ID

EQP322 MAR26 14:17:24 2100 TBL Diag Fail
     NE: 11            LOCATION: 1
     EQP: 1 ABM RFT
     SHELF POS: 1      SHELF: CE
     CPG: Proc B
     SLOT: 21          PEC: NT44K52BC
TC FAIL:               Mate Comms
                       Audit RDL
```

Field descriptions

The following tables explain each of the values that can appear for the TC FAIL field in the EQP322 log report. The failure reasons that appear in the TC FAIL field are dependent on the circuit pack undergoing diagnostics. The column titled “Probable object(s) involved” identifies the most likely causes of the failure; however, for more details, read the action to be taken.

Each of the tables is followed by the actions to be taken.

—continued—

EQP322, continued

Possible TC FAIL reasons for a TAC/MTAC diagnostic

Field	Reason (test)	Possible problem areas	Voltage source
TC FAIL	Card Missing	TAC	not applicable
	Card Mismatch	TAC	not applicable
	IO Card Mismatch	PGTC, TBP, TAP I/O	not applicable
	Tests Aborted	TAC	not applicable
	Card in Reset	TAC	not applicable
	SW Not Loaded	TAC	not applicable
	HW Access Fail	TAC	not applicable
	Int Enable Fail	TAC	not applicable
	Cold Reset Fail	TAC	not applicable
	Cold Reset TmOut	TAC	not applicable
	Diag TmOut	TAC	not applicable
	Vintage-Get Fail	TAC	not applicable
	Loader-Send Fail	TAC	not applicable
	Diag-Send Fail	TAC	not applicable
	Invalid State	TAC	not applicable
	Invalid Res Inst	TAC	not applicable
	PGTCI test	TAC, PGTC, TBP I/O	Talk battery
	Current det	TAC, PGTC, TBP I/O	Talk battery
	TBP I/O	TAC, PGTC, TBP I/O	Talk battery
	MTC Pphone	TAC, PGTC, TBP I/O	Talk battery
	Bad CODEC Calib	TAC	not applicable
	Leak test	TAC	Talk battery
	Continuity	TAC	Talk battery
	TDP test	TAC	not applicable
	A/D test	TAC	Talk battery
	HVG test	TAC	HVG
	LCD test	TAC	Talk battery
	TRC1 and TRC2 test	TAC	HVG
	CODEC test	TAC	Talk battery
	MON1A, 1B, 2A, 2B	TAC	not applicable
	CRO test	TAC	not applicable
	MTAD test	TAC, PGTC, TBP I/O	Talk battery
	MTA tone test	TAC, PGTC, TBP I/O	HVG
	MTA termination	TAC, PGTC, TBP I/O	not applicable
	TBP test	TAC	Talk battery
	MTAC Relay test	MTAC, test cables, bent pins	Talk battery
	Leakage STB1	MTAC, bent pins	Talk battery(from TAC)
	Leakage STB2	MTAC, bent pins	Talk battery(from TAC)
	Continuity	MTAC, test cable connections	Talk battery(from TAC)
	Leakage no STB	MTAC	Talk battery(from TAC)
	Discont. no STB	MTAC	Talk battery(from TAC)
	Discont. STB1	MTAC	Talk battery(from TAC)
	Discont. STB2	MTAC	Talk battery(from TAC)
	Loopback STB1	MTAC	Talk battery(from TAC)
	No loopback STB1	MTAC	Talk battery(from TAC)
	Loopback STB2	MTAC	Talk battery(from TAC)
	No Loopback STB2	MTAC	Talk battery (from TAC)

—continued—

EQP322, continued

Action for TAC diagnostic results

Each of the following headings represents a possible response in the TC fail field of this log report for the test access card (TAC).

Card Missing

The TAC card is missing from its slot. In the empty slot, install a circuit pack bearing the correct product equipment code. Once the TAC has recovered, diagnostics can be repeated.

Card Mismatch

The circuit pack in the slot designated for the test access card does not match the provisioned circuit pack. Replace the mismatched circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

IO Card Mismatch

One of the slots designated for a TAC I/O card (TAP, TBP, or PGTC) houses a card that does not match the provisioned circuit pack. Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code.

Tests Aborted

An activity with higher precedence has caused the TAC diagnostics to abort, for example, insertion or removal of a card in the circuit pack group. Repeat the manual diagnostic request.

Card in Reset
SW Not Loaded
HW Access Fail
Int Enable Fail
Cold Reset Fail
Cold Reset TmOut
Diag

The TAC is in a failed state that is recoverable. The TAC automatically recovers itself by performing a cold reset or software reboot. Therefore, no further action is required.

—continued—

EQP322, continued

Vintage-Get Fail
Loader-Send Fail
Diag-Send Fail
Invalid State
Invalid Res Inst
This failure indicates a severe APU software error that should be accompanied by a SWERR log entry. Re-attempt the TAC diagnostics. If the problem persists, forward this log to Northern Telecom customer support.

Bad CODEC Calib
The calibration values stored in the TAC EPROM are not valid. The TAC is in a “Partial Fail” state. The alarm “TAC Digital Side Unavailable” is raised. Replace the TAC, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

PGTCI test
Current det
TBP I/O
MTC Pphone
Leak test
Continuity
A/D test
LCD test
CODEC test
MTAD test
TBP test
The above tests involve the talk battery. Check to see if the TAC is hooked up to the talk battery, and verify that the talk battery is functioning properly.

HVG test
TRC1 and TRC2 test
MTA tone test
The above tests involve the high-voltage generator on the test access card (TAC). Replace the TAC, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

TDP test
If the TDP test fails, check for an AIC failure. If the AIC is okay, and the CODEC test and MON tests fail as well, replace the TAC, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

—continued—

EQP322, continued

Action for MTAC diagnostic results

Before troubleshooting MTAC failures, check for proper connection of cables and check for bent pins in the line card slots. Make sure line card test relays are not stuck on the drawer test bus, and check for TAC failures.

Determine whether one or two MTACs are failing diagnostics. If only one MTAC is failing, then determine whether the problem is with the MTAC or its slot. If another known-good MTAC is available, perform a swap and recheck the problem. If the problem is still present, or if another MTAC was not available for a swap, check for a loose drawer test bus flex cable or bent pins in the line card slots.

If several MTACs are failing, first check for loose shelf test cables. If all MTACs are still failing, check the TAC for failure. If the TAC is not at fault, replace the MTACs one at a time, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

MTAC Relay test

This diagnostic message is displayed if one or more of the MTAC tests fail diagnostics. To determine the appropriate action, look up the diagnostic messages that appear along with this one.

Leakage STB1
Leakage STB2

Failure of any of the above leakage tests is typically due to bent pins in the line drawer. If none of the drawer pins is bent, check for a loose or defective drawer test bus flex cable located at the back of the drawer, or check for line card test relays that are stuck on the drawer test bus.

Continuity

These results indicate a test bus continuity problem. Typically the problem is a result of loose test cables. Check for proper cable connections daisy-chained between the MTA In and MTA Out connectors on the left side of each copper-distribution shelf. For example, if the MTACs in drawers 2 to 7 have failed, there is a high probability that there is a loose system test bus cable between CDS shelves 1 and 2.

—continued—

EQP322, continued

Discont. no STB
Discont. STB1
Discont. STB2
Leakage no STB
Loopback STB1
Loopback STB2
No Loopback STB1
No Loopback STB2

For any of these failure results, replace the MTAC, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

Possible TC FAIL reasons for a LIC diagnostic

Field	Reason (test)	Possible problem areas
TC FAIL	Data Prov Check	LIC
	Card Access	LIC
	Verify IDPROM	LIC
	Slink Integrity	LIC
	Autonomous Msg	LIC
	Int RX SP Ck	LIC
	Int RX SP Det	LIC
	Reg Read/Write	LIC
	General Sanity	LIC
	Alink TX PP Ck	LIC, LC
	Int TX SP Ck	LIC, LC
	Int TX SP Det	LIC, LC
	Dlnk RX Frame Ck	LIC, VF cable, AIC
	Dlnk RX Frame Dt	LIC, VF cable, AIC
	Dlink RX SP Ck	LIC, VF cable, AIC
	Dlink RX SP Det	LIC, VF cable, AIC
	Dlink TX Frame Dt	LIC, VF cable, AIC
	Dlink TX SP Det	LIC, VF cable, AIC
	Card Presence	LIC, VF cable, AIC

LIC diagnostic results

Each of the following headings represents a possible response in the TC Fail field of this log report for the line interface card (LIC).

Data Prov Check

No action required.

—continued—

EQP322, continued

Card Access
Verify IDPROM,
Slink Integrity
Autonomous Msg
Int RX SP Ck
Int RX SP Det
Reg Read/Write
General Sanity
For these failure reasons, replace the LIC as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

Alink TX PP Ck
Int TX SP Ck
Int TX SP Det
If the LIC is in the TSTF state, replace the LIC, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

If the LIC is not in the TSTF state, replace the line card identified in the log report, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

If replacing the line card does not clear the problem, and the LIC has not yet been replaced, replace the LIC, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

Dlnk RX Frame Ck
Dlnk RX Frame Dt
Dlink RX SP Ck
Dlink RX SP Det
Dlink TX Frame Dt
Dlink TX SP Det
Replace the LIC, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C. If replacing the LIC does not clear the fault, check for proper connection of the VF cables (D-link) from the copper-distribution shelf to the common-equipment shelf.

Card Presence
This failure reason indicates that the LIC is missing, or mismatched, or that there is an access problem between the LIC and the AIC.

—continued—

EQP322, continued

Log into the network element user interface and check for a missing or mismatch alarm raised against the LIC. If a missing or mismatched LIC alarm is present, install a LIC in the missing slot, or replace the mismatched card with the correct line interface card.

If there are no alarms raised against the LIC, check the VF cables (D-link) from the copper-distribution shelf to the common-equipment shelf.

If the VF cables are properly connected, check for alarms raised against the AIC.

Possible TC FAIL reasons for a TIC diagnostic

Field	Reason (test)	Possible problem areas
TC FAIL	Access and ID	TIC, backplane
	Clk fail detect	TIC, OC-12, backplane
	Data path detect	TIC
	TLink failure	TIC, AIC, backplane
	TLink selection	TIC, AIC, backplane
	Inter. and mask	TIC, Proc, backplane
	CBIC reset	TIC
	TBIF reset	TIC
	POP reset	TIC
	CBIC memory	TIC
	TBIF memory	TIC
	POP memory	TIC
	DS0 frame buffer	TIC
	DSIBIF loopback	TIC
	Rx ptr processor	TIC
	STS signal label	TIC
	STS path trace	TIC
	STS perf. mon.	TIC
	STS alarm proc.	TIC
	VT signal label	TIC
	VT perf. mon.	TIC
	VT alarm proc.	TIC
	TBIF mux. demux.	TIC, AIC, backplane
	Sig. phase sync.	TIC
	VT signal freeze	TIC
	DSIBIF frame par	TIC

—continued—

EQP322, continued

TIC diagnostic results

Each of the following headings represents a possible response in the TC Fail field of this log report for the transport interface card (TIC).

CBIC reset
TBIF reset
POP reset
CBIC memory
TBIF memory
POP memory
DS0 frame buffer
DSIBIF loopback
Rx ptr processor
STS signal label
STS path trace
STS perf. mon.
STS alarm proc.
VT signal label
VT perf. mon.
VT alarm proc.
Data path detect
Sig. phase sync.
VT signal freeze
DSIBIF frame par

For any of the above diagnostic failures, replace the TIC as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

Access and ID

Ensure that the TIC is present and properly seated in the shelf slot.

If the TIC is present and properly seated in the shelf slot and continues to fail, replace the TIC, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

—continued—

EQP322, continued

If the TIC continues to fail after being replaced, there may be a problem with the TIC slot or the shelf backplane. Contact your next level of support.

Clk fail detect

If only one TIC fails the diagnostic test, replace the TIC, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

If both TIC A and TIC B fail the diagnostic test, the problem may be with the OC-12, which is the source of the clock. Replace the active OC-12, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

If both TICs continue to fail after replacing the OC-12, there may be a problem with the TIC slot or the shelf backplane. Contact your next level of support.

TLink failure
TLink selection
Inter. and mask
TBIF mux. demux.

Replace the TIC, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

If the TIC continues to fail diagnostics, the problem may be with the AIC. Replace the corresponding (same plane) AIC, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

If the TIC continues to fail diagnostics, there may be a problem with the TIC slot or the shelf backplane. Contact your next level of support.

—continued—

EQP322, continued

Possible TC FAIL reasons for a Proc diagnostic

Field	Reason (test)	Possible problem areas
TC Fail	CBIC Interrupt	Processor
	CBIC VBR	Processor
	CBIC Reset	Processor
	CBIC Autovector	Processor
	CBIC RAM	Processor
	CBIC BIST	Processor
	CBIC Device ID	Processor
	Card IDPROM	Processor
	Flash EEPROM	Processor
	Memory Access	Processor
	Zero Bit Error	Processor
	One Bit Error	Processor
	Two Bit Error	Processor
	HMU Shared Mem	Processor
	HMU Access	Processor
	HMU VBR	Processor
	Invoke HMU Test	Processor
	Shelf ID	Processor
	Verify Clk Fault	Processor
	Verify Sts Area	Processor
	Audit IPC	Processor
	Check OOS Faults	Processor
	Mate Status	Processor
	Shelf IDPROM	Processor, shelf
	CBIC Slv Presence	Processor
	Mate Presence	Processor
	Mate Fail	Processor
	Mate HMU Comms	Processor, bent slot pins
	Mate Comms	Processor, bent slot pins
	Audit RDL	Processor, bent slot pins

—continued—

EQP322, continued

Processor (Proc) diagnostic results

Each of the following headings represents a possible response in the TC Fail field of this log report for the processor (Proc).

CBIC Interrupt
CBIC VBR
CBIC Reset
CBIC Autovector
CBIC RAM
CBIC BIST
CBIC Device ID
Card IDPROM
Flash EEPROM
Memory Access
Zero Bit Error
One Bit Error
Two Bit Error
HMU Shared Mem
HMU Access
HMU VBR
Invoke HMU Test
Shelf ID
Verify Clk Fault

The fail reasons listed above indicate a fault on the processor card. In each case there should be at least one processor alarm raised. Make sure the card is presently the standby. This should have happened automatically. If it did not, perform a switch. Run diagnostics to confirm the failure. If the failure occurs again, replace the Processor card, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

Verify Sts Area

If this test fails, it indicates that the HMU is stuck in firmware. The software should take action automatically. If the software does not take action within 2 minutes of the fault occurring, make sure the failed card is in standby mode, then replace the card.

Audit IPC

If this failure is indicated, the software should take recovery action on its own. Check for processor alarms, and clear them as indicated in *Alarm and Trouble Clearing Procedures,* 323-3001-543 in *Maintenance,* Volume 5A. If this failure does not clear after 2 minutes, and there are no processor alarms, make sure the processor is in standby mode, then replace the processor, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

—continued—

EQP322, continued

Check OOS Faults

This failure indicates that there are out-of-service (OOS) faults on the processor. Make the processor standby, then take the processor out of service. Run diagnostics to either clear the OOS faults or confirm them. Perform action based on the test that fails, or check alarms, and perform action as indicated in *Alarm and Trouble Clearing Procedures,* 323-3001-543 in *Maintenance,* Volume 5A.

Mate Status

This failure may indicate a failure on or off the processor card. Run diagnostics on both processors to determine if a more serious problem exists. If a failure occurs on one processor card, replace that card, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C. If other failures occur, follow actions for the other failure first, then diagnose both processors again.

Shelf IDPROM
CBIC Slv Presenc

This failure indicates either a problem with the CBIC on the processor card or a problem with the shelf ID EEPROM circuitry. If the problem is with the shelf, the failure should show up on both processors after running diagnostics on both. Shelf failures should be reported to your next level of support. If the failure is related to the processor card, the processor card identified by the log needs replacing, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

Mate Presence

This failure indicates that the standby processor is not inserted or that there is a problem with the mate presence circuitry on one of the two processors. If the standby processor is inserted and this failure occurs when running diagnostics, replace the standby processor, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C. If the failure is still indicated after the standby processor downloads, then the problem is in the active processor, which must be replaced, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

> ***Note:*** A protection switch may not work properly, so an active card may have to be pulled. This can be service-affecting.

Mate Fail

This failure indicates that the standby processor has failed. This failure can stay active while a processor is downloading. If the failure persists after downloading is complete, replace the standby processor, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

—continued—

EQP322, continued

Mate HMU Comms
Mate Comms
Audit RDL

These failures indicate problems with the interprocessor communication. If diagnostics are run on the standby processor while it is loading software, one or more of these failures will occur. Before taking any action, ensure that the standby processor is not downloading. Downloading, which can take several minutes, is indicated by the INIT LED on the circuit pack. If the standby processor is not downloading, and one of these faults persists, replace the standby processor card, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C. If the problem persists after replacing the standby processor card, replace the active processor, as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C. If this again does not solve the problem, there may be bent pins on one of the processor slots. If bent pins are the cause, contact your next level of support.

—end—

EQP323

Report explanation

This log report indicates that either a node type change (NTC) or a redundancy type change (RTC) has failed.

Report example

The following is an example of an EQP323 log report for a NTC failure:

```
      EQP323 OCT31 20:35:20 2300 TBL TC Failure
REASON: Serial Telemetry Restriction
Parameter Changed: Eqpt Type
Present Value: LTE
Target Value: ADM
      NE:632 LOCATION: 1
      EQP: 1 OC12 Terminal
      SHELF POS: 1 SHELF: 1
      MEMBER: OC12 G1
```

The following is an example of an EQP323 log report for a RTC failure:

```
      EQP323 OCT31 20:35:20 2300 TBL TC Failure
REASON: OC12appAUnexpect
Parameter Changed: Protection Scheme
Present Value: plus (+)
Target Value: colon (:)
Parameter Changed: Revertive Indicator
Present Value: Non-revertive
Target Value: Revertive
Parameter Changed: Number Of Protected
Present Value: 1
Target Value: 3
      NE:632 LOCATION: 1
      EQP: 1 OC12 Terminal
      SHELF POS: 1 SHELF: 1
      MEMBER: OC12 G1
```

—continued—

EQP323, continued

Field descriptions

The following table provides information on the generic format used for both NTC and RTC. These fields always appear for both NTC and RTC. For the RTC there can be more than one occurrence of the Parameter Changed, Present Value, and Target Value fields.

Field	Value	Description
REASON	ASCII string	Name of the application that failed
Parameter Changed	Protection Scheme (for RTC) Eqpt Type (for NTC)	Identifier of the attribute that the change was attempted on
Present Value	ASCII string	Current value of the attribute
Target Value	ASCII string	Value of the attribute that the change was attempted on
NE	1 to 32767	Network element number
LOCATION	ASCII string	Frame name
EQP	ASCII string	Equipment identification
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
MEMBER	ASCII string	Identifier of a protection group member

—continued—

EQP323, continued

The following table provides information on the Parameter Changed field for NTC.

Parameter Changed	Present Value or Target Value	Optional	Description
Eqpt Type	ACOT ADM BLSR DCOT FCOT IDT LTE Network_cntrl_node OC48 LTE OC48 STE Radio Switch Node RDT RFT RPTR	no	Operating mode of the node

The following table provides information on the Parameter Changed field for RTC.

Parameter Changed	Present Value or Target Value	Optional	Description
Protection Scheme	plus (+) colon (:)	no	Type of protection scheme
Revertive Indicator	Revertive Nonrevertive	yes	Revertive indicator for the protection scheme
Number Of Protected	0 to 999	yes	Number of protected elements
Number Of Protecting	0 to 999	yes	Number of protecting elements
Route Diversity	On Off	yes	Toggle for routing diversity
Switch Mode	unidirectional bidirectional	yes	Type of switching mode

—continued—

EQP323, continued

Action

Step	Action
1	Investigate the states of the node type or redundancy type for the cause of the failure.
2	For further information, see *Alarm and Trouble Clearing Procedures*, 323-3001-543 in *Maintenance*, Volume 5A, for the appropriate action.

—end—

EQP324

Report explanation

This log report is generated if a state change fails or is aborted.

Report example

The following is an example of an EQP324 log report:

```
      *  EQP324 OCT30 23:14:34 8800 TBL Diag Fail
      NE:704             LOCATION: 1
      EQP: 1 OC12 RingADM
      SHELF POS: 1       SHELF: 1
      CPG: Proc A
      SLOT: 21     PEC: NT4K52BC
TC FAIL: HMU VBR
```

Field descriptions

Field	Value	Description
Object Class	ASCII string	Object that failed/denied the protection request
Operation	Failed Denied	State of the switch attempt
Reason	Force (Local) Manual (Local) Signal/Eqp Fail (Local) Signal Degrade (Local)	Protection operation that failed or was denied
NE	1 to 32767	Network element number
LOCATION	ASCII string	Frame name
EQP	ASCII string	Equipment identification
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
MEMBER	ASCII string	Identifier of a protection group member.
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code
TC FAIL	ASCII string	Reason for failure

—continued—

EQP324, continued

Action

Step	Action
1	For further information, see *Alarm and Trouble Clearing Procedures*, 323-3001-543 in *Maintenance*, Volume 5A, for the appropriate action.

—end—

EQP326

Report explanation

A diagnostic was aborted due to a higher priority change of state.

Report format

The following is the format for log report EQP326.

EQP326 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: <class>
Reason: <reason>
Previous State: <previous>
Present State: <present>
Location fields. See Appendix A.

Report example

The following shows a typical example of log report EQP326.

```
EQP326 DEC26 23:07:11 9700 TBL State Change Fail
Object Class: Circuit Pack Group
Reason: Abort
Previous State:
Present State:
       NE: 12             LOCATION: 1 MARK 12
       EQP: 1 ABM RFT
       SHELF POS: 2       SHELF: CDS 1
       CPG: NLIC A        SLOT: 12
```

Field descriptions

The following table lists the object classes in this log report.

Field	Value	Description
<class>	Equipment Frame Shelf Circuit Pack Circuit Pack Group Member Redundancy Group Redundancy Group Member	Object that was failed

—continued—

—continued—

EQP326, continued

Field	Value	Description
<reason>	Abort	Reason why diagnostic failed
<previous>	IS, OOS	State of object before diagnostic failure
<present>	OOS, IS	State of object after diagnostic failure

—end—

Action

Repeat diagnostic.

—end—

EQP329

Report explanation

This log report indicates that a ring protection switch request has failed or been denied due to a problem with the protection path over which the switch was to occur.

Report example

The following is an example of an EQP329 log report:

```
      * EQP329 NOV16 17:19:53 7300 TBL Ring Protection Activity
Object Class: Redundancy Group Member
Operation: Failed
Reason   : Forced (Local)                Reached NE: 32
Switch Fail Reason: Conflict-sigFail
      NE:12 Toronto      LOCATION: 1 Row A
      EQP: 1 OC12 RingADM
      SHELF POS: 1       SHELF: 1
      MEMBER: OC12 G1
      SLOT:9       PEC: NT7E02KC
```

—continued—

EQP329, continued

Field descriptions

Field	Value	Description
Object Class	ASCII string	Object that failed/denied the protection request
Operation	Failed Denied	State of the switch attempt
Reason	Forced (Local)/(Remote) Manual (Local)/(Remote) Signal/Eqp Fail (Local) Signal Degrade (Local)	Protection operation that failed or was denied
Reached NE	1 to 32767	Neighbor Network element number
Switch fail reason	Conflict-sigFail Conflict-manual Unexpected APS code	Some examples of reasons the switch failed
NE	1 to 32767	Network element number
LOCATION	ASCII string	Frame name
EQP	ASCII string	Equipment identification
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
MEMBER	ASCII string	Identifier of a protection group member
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code

Action

Step	Action
1	Investigate the states of the redundancy group members for the cause of failed or denied protection.
2	For further information, see *Alarm and Trouble Clearing Procedures*, 323-3001-543 in *Maintenance*, Volume 5A, for the appropriate action.

—end—

EQP331

Report explanation

This log report indicates the clock mode has been in holdover for more than 24 hours.

Report example

The following is an example of an EQP331 log report:

```
      EQP331 NOV16 19:22:46 2300 INFO Data Change
Object Class:Clock Mode (Timing Filter Mode)
Reason:  Clock Mode Stayed in Holdover
                   for 24 hours
      NE: 51              LOCATION: 1
      EQP: 1 OC12RingADM
      SHELF POS: 1        SHELF: 1
      CPG: OC12 G1
      SLOT: 9      PEC: NT7E05BC
```

Field descriptions

Field	Value	Description
Object Class	Clock Mode (Timing Filter Mode)	Class of the object
Reason	ASCII string	Clock mode has been in holdover for more than 24 hours
NE	1 to 32767	Network element number
LOCATION	ASCII string	Frame name
EQP	ASCII string	Identifier of the created/deleted object
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
CPG	ASCII string	Circuit pack group identifier
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code

Action

No action is required. This log is for information only.

—end—

EQP401

Report explanation

This log report indicates the successful creation or deletion of an object within the system.

Creation applies to the following objects:

- Equipment
- Frame
- Shelf
- Circuit Pack Group
- Circuit Pack
- Redundancy Group
- Redundancy Group Member
- ESI Circuit Pack Group
- Clock Mode

Deletion applies to the following objects:

- Circuit Pack Group
- Redundancy Group
- Redundancy Group Member
- Clock Mode

Report format

The following is the format for log report EQP401.

EQP401 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: <class>
Location fields. See Appendix A.

—continued—

EQP401, continued

Report example

The following shows a typical example of log report EQP401.

```
EQP401 MAR26 23:00:00 9700 INFO Delete
Object Class: Circuit Pack Group
Operation: Delete
       NE: 12
       EQP: 1 ABM FCOT
       SHELF POS: 2      SHELF: CDS 1
       CPG: NLIC B       SLOT: 98
```

The following are EQP401 log examples of a Circuit Pack Group creation and a Redundancy Group Member deletion for both DS1 and STS-1 configurations:

Circuit Pack Group creation—DS1:

```
       EQP401 MAR26 15:44:10 2500 INFO Create/Delete
Object Class: Circuit Pack Group
Operation: Create
       NE: 661 LOCATION: 1
       EQP: 1 TBM FCOT
       SHELF POS: 1 SHELF: 1
       CPG: DS1 G12
       SLOT: 18 PEC: NT7E04AA
       SLOT: 51 PEC: NT4K32AA
       SLOT: 53 PEC: NT4K33AA
       State: IS
```

Circuit Pack Group creation—STS-1:

```
       EQP401 APR21 19:57:58 3400 INFO Create/Delete
Object Class: Circuit Pack Group
Operation: Create
       NE: 35 LOCATION: 1
       EQP: 1 OC12 RingADM
       SHELF POS: 1 SHELF: 1
       CPG: STS1 G2
       SLOT: 13 PEC: NT7E09AA
       SLOT: 42 PEC: NT4K30AA
       SLOT: 43 PEC: NT4K30AA
       SLOT: 44 PEC: NT4K30AA
       STATE: IS
```

—continued—

EQP401, continued

Redundancy Group Member deletion—DS1:

```
       EQP401 MAR26 15:44:10 2300 INFO Create/Delete
Object Class: Redundancy Group Member
Operation: Delete
       NE: 661 LOCATION: 1
       EQP: 1 TBM FCOT
       SHELF POS: 1 SHELF: 1
       MEMBER: DS1 G12
       SLOT: 18 PEC: NT7E04AA
       SLOT: 51 PEC: NT4K32AA
       SLOT: 53 PEC: NT4K33AA
```

Redundancy Group Member deletion—STS-1:

```
       EQP401 APR21 19:57:59 3500 INFO Create/Delete
Object Class: Redundancy Group Member
Operation: Delete
       NE: 35 LOCATION: 1
       EQP: 1 OC12 RingADM
       SHELF POS: 1 SHELF: 1
       MEMBER: STS1 G2
       SLOT: 13 PEC: NT7E09AA
       SLOT: 42 PEC: NT4K30AA
       SLOT: 43 PEC: NT4K30AA
       SLOT: 44 PEC: NT4K30AA
```

—continued—

EQP401, continued

Field descriptions

The following table lists the object classes in this log report.

Field	Value	Description
Object Class	Equipment Frame Shelf Circuit Pack Circuit Pack Group Member Redundancy Group Redundancy Group Member	Class of the created/deleted object
Operation	Create Delete	Operation performed
NE	1 to 32767	Network element number
LOCATION	ASCII string	Frame name
EQP	ASCII string	Equipment identification
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
CPG	ASCII string	Circuit pack group
MEMBER	ASCII string	Identifier of a protection group member
State	IS IS TRBL OOS OOS MTC	Valid only for Circuit Pack Group Create; the state in which the CPG was created
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code

Action

No action is required. This log is for information only.

—end—

EQP403

Report explanation

This log report indicates an object instance attribute change was performed successfully. This category also includes the successful completion of redundancy type changes (RTC).

It is also generated whenever the exerciser is inhibited or enabled for an optics protection group. When the EQP403 log reports an inhibited result it means the exerciser cannot perform a test because the equipment is connected to the equipment of another manufacturer. Therefore, the test is “inhibited” because the exerciser cannot recognize the other equipment.

Report example

The following are examples of EQP403 log reports for an object instance attribute change:

```
      EQP403 NOV16 15:27:50 3300 INFO Data Change
Object Class: Equipment
Parameter Changed: Time of Day
Present Value: 1994/11/16 15:27:50.147
Previous Value: 1994/11/16 15:22:02.805
      NE: 632            LOCATION: 1
      EQP: 1 OC12 Terminal

      EQP403 NOV16 19:22:46 4900 INFO Data Change
Object Class: Circuit Pack Group
Parameter Changed:  REX Enable
Present Value: Off
Previous Value: On
      NE: 36             LOCATION: 1
      EQP: 1 OC12RingADM
      SHELF POS: 1       SHELF: 1
      CPG: Proc A
      SLOT: 21     PEC: NT4K52BB

      EQP403 NOV16 19:22:46 2300 INFO Data Change
Object Class: Clock Mode (Timing Filter Mode)
Parameter Changed:  Target Clock Mode
Present Value: Holdover
Previous Value: Normal
      NE: 51             LOCATION: 1
      EQP: 1 OC12RingADM
      SHELF POS: 1       SHELF: 1
      CPG: OC12 G1
      SLOT: 9      PEC: NT7E05BC
```

—continued—

EQP403, continued

The following is an example of an EQP403 log report for a successful RTC:

```
      EQP403 OCT26 14:24:19 1000 INFO Data Change
Object Class: Redundancy Group
Parameter Changed:Protection Scheme
Present Value:plus (+)
Previous Value:colon (:)
Parameter Changed: Revertive
Present Value: Yes
Previous Value: No
Parameter Changed: Number Of Protected
Present Value: 3
Previous Value: 1
      NE: 632 LOCATION: 1
      EQP: 1 OC12 Terminal
      SHELF POS: 1 SHELF: 1
      MEMBER: OC12 G1
```

The following are examples of an EQP403 log when the exerciser is inhibited and enabled:

EQP403 log generated when the exerciser is inhibited:

```
      EQP403 FEB07 12:57:37 1300 INFO Data Change
Object Class: Redundancy Group
Parameter Changed: Protection Exerciser
Present Value: Inhibited
Previous Value: Enabled
      NE: 22            LOCATION: 1
      EQP: 1 OC12 Terminal
      SHELF POS: 1      SHELF: 1
      MEMBER: OC12 G1
```

EQP403 log generated when the exerciser is enabled:

```
      EQP403 FEB14 10:32:53 1700 INFO Data Change
Object Class: Redundancy Group
Parameter Changed: Protection Exerciser
Present Value: Enabled
Previous Value: Inhibited
      NE: 22            LOCATION: 1
      EQP: 1 OC12 Terminal
      SHELF POS: 1      SHELF: 1
      MEMBER: OC12 G1
```

—continued—

EQP403, continued

Field descriptions

Field	Value	Description
Object Class	ASCII string	Class of the created/deleted object
Parameter Changed	ASCII string	Identifier of the attribute that changed
Present Value	YYYY/MM/DD hh:mm:ss, On or Off, Normal, Holdover, or Freerun plus (+) or colon (:), Inhibited or Enabled	Current value of the attribute
Previous Value	YYYY/MM/DD hh:mm:ss, On or Off, Normal, Holdover, or Freerun plus (+) or colon (:), Inhibited or Enabled	Value of the attribute before the change
NE	1 to 32767	Network element number
LOCATION	ASCII string	Frame name
EQP	ASCII string	Identifier of the created/deleted object
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
CPG	ASCII string	Circuit pack group identifier
MEMBER	ASCII string	Identifier of a protection group member
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code

—continued—

EQP403, continued

The following table provides information on the Parameter Changed field for RTC.

Parameter Changed	Present Value or Target Value	Optional	Description
Protection Scheme	plus (+) colon (:)	no	Type of protection scheme
Revertive Indicator	Revertive Non-revertive	yes	Revertive indicator for the protection scheme
Number Of Protected	0 to 999	yes	Number of protected elements
Number Of Protecting	0 to 999	yes	Number of protecting elements
Route Diversity	On Off	yes	Toggle for routing diversity
Switch Mode	unidirectional bidirectional	yes	Type of switching mode

Action

No action is required. This log is for information only.

—end—

EQP501

Report explanation

This log report indicates manual state changes within the system. An object instance’s state was changed through a manual request.

Report format

The following is the format for log report EQP501.

EQP501 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: Object Class
Present State: Pres State
Previous State: Prev State

Report example

The following shows a typical example of log report EQP501.

```
EQP501 NOV26 17:02:41 1000 INFO State Change
Object Class: Circuit Pack Group
Present State: OOS
Previous State: IS
     NE: 661                  LOCATION: 1
     EQP: AccessNode
     SHELF POS: 1             SHELF: 1
     CPG: DS1       G3
     SLOT: 5 6      PEC: NT7E02KC
```

The following are examples of an EQP501 log report for an OC-12 and STS-1 state change:

```
       EQP501 NOV16 17:13:45 6800 INFO State Change
Object Class: Circuit Pack Group
Present State: IS
Previous State: OOS
       NE: 12 Ring5 LOCATION: 1 TORONTO
       EQP: 1 OC12 RingADM
       SHELF POS: 1 SHELF: 1
       CPG:OC12 G1
       SLOT: 9 PEC: NT7E05BG
```

—continued—

EQP501, continued

```
       EQP501 APR21 19:48:09 2000 INFO State Change
Object Class: Circuit Pack Group
Present State: OOS
Previous State: IS
       NE: 35 LOCATION: 1
       EQP: 1 OC12 RingADM
       SHELF POSITION: 1 SHELF: 1
       CPG: STS1 G2
       SLOT: 13 PEC: NT7E09AA
       SLOT: 42 PEC: NT4K30AA
       SLOT: 43 PEC: NT4K30AA
       SLOT: 44 PEC: NT4K30AA
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
Object Class	ASCII string	Class of the object that changed state
Pres State	OOS MTC OOS IS IS TRBL	The current state of the object
Prev State	IS TRBL IS OOS OOS MTC	The previous state of the object
NE	1 to 32767	Network element identifier
LOCATION	ASCII string	Frame name
EQP	ASCII string	Equipment identification
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
CPG	ASCII string	Circuit pack group identifier
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code

Action

No action is required. This log is for information only.

—end—

EQP606

Report explanation

This log report indicates that a protection activity was performed or released successfully, or was preempted due to a higher priority activity, or went into a wait-to-restore period upon release.

Report format

The following is the format for log report EQP606.

EQP606 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: Object Class
Operation: Operation
Reason: Reason

Report example

The following shows a typical example of log report EQP606.

```
EQP606 MAR26 14:16:06 1800 INFO Protection Activity
Object Class: Redundancy Group Member
Operation: Operate
Reason: Manual (Local)
     NE: 661            LOCATION: 1
     EQP: AccessNode
     SHELF POS: 1       SHELF: 1
     MEMBER: DS1 G1
     SLOT: 10           PEC: NT7E02KC
```

The following are examples of an EQP606 log report for OC-12 and STS-1 protection activity:

```
       EQP606 NOV15 18:59:05 1400 INFO Protection Activity
Object Class: Redundancy Group Member
Operation: Operate
Reason:Signal/Eqp Fail (Local)
       NE:9 LOCATION: 1
       EQP: 1 OC12 RingADM
       SHELF POS: 1 SHELF: 1
       MEMBER:OC12 G2
       SLOT: 10 PEC: NT7E02BG
```

—continued—

EQP606, continued

```
       EQP606 APR21 19:20:00 1600 INFO Protection Activity
Object Class: Redundancy Group Member
Operation: Operate
Reason: Forced (Local)
       NE: 35 LOCATION: 1
       EQP: 1 OC12 RingADM
       SHELF POS: 1 SHELF: 1
       MEMBER: STS1 G1
       SLOT: 11 PEC: NT7E09AA
       SLOT: 38 PEC: NT4K30AA
       SLOT: 39 PEC: NT4K30AA
       SLOT: 40 PEC: NT4K30AA
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
Object Class	ASCII string	Class of the object class that failed/denied the protection request
Operation	Operate Release Preempt	Protection operation performed
Reason	Auto (Local) Auto (Remote) Force (Local) Force (Remote) Lockout (Local) Lockout (Remote) Manual (Local) Manual (Remote) Signal/Eqp Fail (Local) Signal/Eqp Fail (Remote) Signal Degrade (Local) Signal Degrade (Remote) STS1 PathOverhead switch Wait to restore (Local) Wait to restore (Remote)	Type of protection operation that was performed, released or pre-empted. Note: an STS1 PathOverhead switch will only generate this log when performed (not upon a release).
NE	1 to 32767	Network element identifier
LOCATION	ASCII string	Frame name
EQP	ASCII string	Equipment identification

—continued—

—continued—

EQP606, continued

Field	Value	Description
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
MEMBER	ASCII string	Identifier of a protection group member
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code
—end—		

Action

No action is required. This log is for information only.

—end—

EQP608

Report explanation

This log provides results of the exerciser when invoked from the Shelf UI screen, or through the scheduler.

Report format

The following is the format for log report EQP608.

```
EQP608 mmm:dd hh:mm:ss nnnn event_type event_label
NE: <ne>                          LOCATION: <location>
EQP: <eqp>
<resource>: <results>
```

Report example

The following shows a typical example of log report EQP608.

```
EQP608 MA26 15:17:47 2400 INFO Exerciser Results
NE: 661                  LOCATION: 1
EQP: AccessNode
OC12: passed
OC3 G1S: inhibited
STS1 G1: passed
DS3 G2: passed
DS3 G3: NOT RUN
DS1 G11: passED
DS1 G12: passed
TXC G2: passed
Field descriptions
```

The following table explains each of the fields in this log report.

Field	Value	Description
<resource>	DS1, DS3 OC3, OC12 Proc, TXC	Identifies the resource
<results>		Identifies the results of the exerciser operation run on a per resource basis:
	pass fail not run	– The exerciser was successful. – The exerciser failed. – The exerciser was not run due to state restrictions on the exercised resource.

Action

None

—end—

EQP609

Report explanation

This log report indicates the successful completion of a manual diagnostic test.

Report format

The following is the format for log report EQP609.

EQP609 mmm:dd hh:mm:ss nnnn event_type event_label

Report example

The following shows a typical example of log report EQP609.

```
EQP609 JUL20 16:49:37 5100 INFO Diag Pass/Abort
NE: 192               LOCATION: 1
EQP: 1 ABM RFT
SHELF POS: 1          SHELF: CE
CPG: OC12 G1
SLOT: 9 PEC: NT7E02KC
Result: Diag Pass
```

Field descriptions

The fields of this log indicate the equipment upon which the manual diagnostic was run. For details on the possible fields, see “Log location fields”, in Appendix A.

Action

None

—end—

EQP610

Report explanation

This log report indicates, as well as provides reasons for, a time of day synchronization failure.

Report format

The following is the format for log report EQP610.

EQP610 mmm:dd hh:mm:ss nnnn event_type event_label
Failed Operation: <failed operation>
Reason: <reason text>

Report example

The following shows a typical example of log report EQP610.

```
EQP610 DEC26 15:17:47 2400 TBL TOD failed
Failed Operation: TOD Synchronization
Reason: Unable to reach OPC
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<failed operation>	TOD Synchronization	The Time of Day synchronization failed.
<reason>	Unable to reach OPC	Communication with the OPC is down.
	Bad time/date received	Invalid time or date was received from the OPC.
	Unable to set clock	Clock could not be set at the NE.

Action

If the reason field indicates Unable to reach OPC, check the status of the OPC and contact Northern Telecom support.

If the reason field indicates Bad time/date received, contact NT support.

If the reason field indicates Unable to set clock, try replacing the maintenance interface card (MIC). If the problem continues, contact NT support.

—end—

EQP612

Report explanation

This log provides the result of a manual REX when invoked from the corresponding circuit pack group screen.

Report format

The following is the format for EQP612 log report.

```
EQP612 mmm:dd hh:mm:ss nnnn event_type event_label
Manual REX result: <rex result>
NE: <ne>                    LOCATION: <location>
EQP: <eqp>
Shelf Pos: <shelf pos>      Shelf: <shelf>
CPG: <cpg>                  Slot: <slot>
```

Report example

The following shows a typical example of EQP612 log report.

```
EQP612 MAY12 12:34:56
Manual REX result: fail
NE: 661 Ottawa           Location: 1 Frame1
EQP: 1 AccessNode
Shelf Pos: 3             Shelf: 1
CPG: Proc A              Slot: 17
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<rex result>	fail abort pass	Result of the REX test
<ne>	integer	Network element
<location>	alphanumeric	The frame name
<eqp>	AccessNode	Equipment type
<shelf pos>	integer	Shelf position
<shelf>	integer	Shelf position within the frame

—continued—

—continued—

EQP612, continued

Field	**Value**	**Description**
<cpg>	Alphanumeric	circuit pack group
<slot>	integer	Slot number in the shelf

—end—

Action

None

—end—

EQP613

Report explanation

This log indicates that a diagnostic test could not be run. The details are indicated by the text string in the reason field.

Report format

The following is the format for log report EQP613.

EQP613 mmm:dd hh:mm:ss nnnn event_type event_label
REASON: <reason>
Location fields. See Appendix A.

Report example

The following shows a typical example of log report EQP613.

```
EQP613 MAY12 12:34:56 INFO Diag Not Run
REASON: TAC unavailable
NE: 11                   Location: 1
EQP: 1 ABM RFT
SHELF POS: 2             SHELF: CDS
CPG: MTAC A
```

Field descriptions

Field	Value	Description
<reason>	TAC unavailable	TAC is unable to perform one of the tests.
	CODEC unavailable	TAC or MTAC has reserved this resource.
	STB1 unavailable	TAC or MTAC has reserved this resource.
	STB2 unavailable	TAC or MTAC has reserved this resource.
	Resources reserved	MTAC has reserved the resources or this MTAC diagnostic session has been aborted due to parent equipment failure.

Action

The action for each of the reasons, is listed below:

TAC unavailable

No action required. Wait until the TAC is in-service and retry the MTAC diagnostics.

—continued—

EQP613, continued

CODEC unavailable

No action required. Wait until the TAC is in-service and no other MTAC is running diagnostics, then try again.

STB1 unavailable

No action required. Wait until the TAC is in-service and no other MTAC is running diagnostics, then try again.

STB2 unavailable

No action required. Wait until the TAC is in-service and no other MTAC is running diagnostics, then try again.

Resources reserved

No action required. Wait until the TAC is in-service and no other MTAC is running diagnostics, or has parent equipment failure, then try again.

—end—

EQP617

Report explanation

This log report indicates one of three conditions: that a ring protection activity was performed or released successfully, it was preempted due to a higher-priority activity, or it went into a wait-to-restore period upon release.

Report example

The following shows an example of an EQP617 log report:

```
      EQP617 NOV16 17:18:09 7000 INFO Ring Protection Activity
Object Class: Redundancy Group Member
Operation: Operate
Reason: Lockout Working (Local)          Reached NE: 13
      NE:12 Ring5        LOCATION: 1 TORONTO
      EQP: 1 OC12 RingADM
      SHELF POS: 1       SHELF: 1
      MEMBER: OC12 G1
      SLOT:9       PEC: NT7E02KC
```

—continued—

EQP617, continued

Field descriptions

Field	Value	Description
Object Class	ASCII string	Class of the object that failed/denied the protection request
Operation	Operate Release Preempt	Operation performed
Reason	Force (Local) Force (Remote) Lockout (Local) Lockout (Remote) Manual (Local) Manual (Remote) Signal/Eqp Fail (Local) Signal/Eqp Fail (Remote) Signal Degrade (Local) Signal Degrade (Remote) Wait to restore (Local) Wait to restore (Remote)	Protection operation that was performed, released, or preempted
Reached NE	1 to 32767	Neighbor Network element number
NE	1 to 32767	Network element number
LOCATION	ASCII string	Frame name
EQP	ASCII string	Equipment identification
SHELF POS	1, 2, or 3	Position of shelf
SHELF	1	Shelf identifier
MEMBER	ASCII string	Identifier of a protection group member
SLOT	Integer value	Slot affected
PEC	Alphanumeric string	Product engineering code

Action

No action is required. This log is for information only.

—end—

EVNT301

Report explanation

All event reports are queued for delivery, against a routing system called the discriminator. A finite amount of storage space is allocated for each of the different types of event reports for queueing reports prior to their delivery. If any of these queues is filled to capacity, subsequent reports for which no storage can be found are discarded. All reports discarded are counted and a log of this type is issued after every report delivery.

The side effects are as follows:

alarms
The Log/Alarm system (LAS) on the OPC will fail to receive some alarm reports. It will bring itself up to date eventually when the audit task runs.

logs
The indicated number of logs were not sent to the OPC.

attribute changes
UI screen updates may go missing, putting either OPC or NE UIs out of date or incorrect (reselect or update screen). The Network banner on the OPC may lose an update so the network alarm counts will be inaccurate. They will be corrected automatically by periodic audit.

enrolls/deenrolls
Enrolls do not affect much of anything due to UI design. Loss of deenrolls will prevent posting the “Object deleted” message on a UI screen following a delete operation.

Report format

The following is the format for log report EVNT301.

```
EVNT301 mmm:dd hh:mm:ss nnnn event_type event_label
Discriminator input buffer overflow
alarm reports lost = <number of alarms>
log reports lost = <number of logs>
attribute changes lost = <number of attributes>
enrolls/deenrolls lost = <number of notification reports>
```

—continued—

EVNT301, continued

Report example

The following shows a typical example of log report EVNT301.

```
EVNT301 FEB11 16:41:51 0700 INFO Reports lost
Discriminator input buffer overflow
alarm reports lost = 0
log reports lost   = 0
attribute changes lost = 7
enrolls/deenrolls lost = 0
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<number of alarms>	Integer (indicates number of reports lost since last report was delivered).	Alarm reports lost when attempting to queue them on the delivery process for routing and delivery.
<number of logs>	Integer (indicates number of reports lost since last report was delivered).	Log reports lost when attempting to queue them on the delivery process for routing and delivery.
<number of attributes>	Integer (indicates number of reports lost since last report was delivered).	Attribute change (e.g., screen updates) lost when attempting to queue them on the delivery process for routing and delivery.
<number of notification reports>	Integer (indicates number of reports lost since last report was delivered).	Object create/delete notification reports lost when attempting to queue them on the delivery process for routing and delivery.

Note: “last report” means the last report of ANY type, not necessarily the type that was lost.

—continued—

EVNT301, continued

Action

The action to take depends on the event that was lost.

Alarm reports lost

To rectify or alleviate the problem of missing alarms, try the following:

1. Wait until the log/alarm system (LAS) audit runs and the system corrects itself. This will take 5 minutes for each NE in the OPC span of control.
2. Access the local user interface and observe the alarms. This will enable the craftperson to see the alarms immediately without performing a restart. The audit will eventually bring the OPC back into synchronization with the NE.
3. Perform a warm restart on the NE reporting this log.

Log reports lost

No action possible. For information only.

Attribute changes lost

Redisplay any visible user interface screens to make sure that the most current data is displayed.

Enrolls/deenrolls lost

Redisplay any visible user interface screens to make sure that the most current data is displayed.

—end—

EVNT302

Report explanation

A failure prevented the discriminatory routing process from sending the indicated type of report. The reason why the operation failed is displayed in the reason text.

Process dead The command handling process (which routes all messages) died and has yet to be resurrected. The report will be sent when the process comes back.

Assoc. Down The association the report was supposed to be sent on went down; the message has been discarded.

Bad Message A problem was encountered when trying to format the message; the message has been discarded.

Flow Control Some level of the communications path is overloaded and has requested a stoppage of event shipping until the backlog can be processed. (Note: this measure does not apply to FWP04.)

Internal Fail A lack of memory was encountered when the discriminatory routing process was trying to format a report. Alternatively, the command handler failed to get an invoke id for the message, indicating that the system message limit has been reached. The message will be shipped when either condition is alleviated.

Report format

The following is the format for log report EVNT302.

EVNT302 mmm:dd hh:mm:ss nnnn event_type event_label
Discriminator send_report failed
Report type = <type>
Reason = <reason>

Report example

The following is a typical example of log report EVNT302.

```
EVNT302 FEB11 16:41:51 0700 INFO Send Fail
Discriminator send_report failed
Report type = alarm
Reason = assoc. down
```

—continued—

EVNT302, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<type>	alarm attchng log enroll	Indicates the type of report that failed to be sent.
<reason>	Process Dead Assoc. Down Bad Message Flow Control Internal Fail	Reason why the report could not be sent. See the “Report Explanation” section at the beginning of this log for definitions of each reason.

Action

There are no user actions that can be performed other than to reduce the demands on the system. Demands can be reduced by logging out some local user interfaces on the NE reporting the problem. The CPU load can be reduced by halting any diagnostics or exerciser test running when the reporting problem occurred.

—end—

FAC401

Report explanation

This log report indicates that a successful attribute change has occurred on a termination. This log can appear for the following facilities: DS1, DS3, OC-3, OC-12, STS-1, or ESI.

Report format

The following is the format for log report FAC401.

```
FAC401 mmm:dd hh:mm:ss nnnn event_type event_label
Facility type: <type>
Parameter Changed: <param chgd>
Present value: <pres val>
Previous value: <prev val>
CLFI: <clfi>
     NE: <ne>            EQP: <eqp>
     LOCATION: <pos>
     Shelf: <shelf>      CPG: <cpg>      Port: <port>
```

Report example

The following shows typical examples of a FAC401 log report.

```
FAC401 MAR23 21:42:23 0200 INFO Data Changed
Facility type: DS1
Parameter changed: Loopback
Present value: Term
Previous value: None
CLFI:
     NE: 35              EQP: DS1
     LOCATION:           POS: 2
     Shelf: 1            CPG: G1         Port: 2


FAC401 NOV06 21:08:01 9700 INFO Data Changed
Facility type: ESI
Parameter changed: AIS Quality Lvl Threshold
Present value: SONET Internal Clock
Previous value: Stratum 3
CLFI:
NE:636                   EQP:ESI
LOCATION:                POS: 1
Shelf: 1                 CPG:G1          Port:--
```

—continued—

FAC401, continued

The following are examples of a FAC401 log report for a DS3 and an STS-1 Facility type. (See the “Field descriptions” table on page FAC-4 for further information).

```
       FAC401 MAR23 21:42:23 0200 INFO Data Changed
Facility type: DS3
Parameter changed: Common Language Fac Id
Present value: ST1
Previous value: ST2
CLFI: PAUL
       NE: 35 EQP: DS3
       LOCATION: POS: 2
       Shelf: 1 CPG: G1 Port: 2

       FAC401 APR21 20:03:56 3800 INFO Data Changed
Facility type: STS1
Parameter changed: Loopback Type
Present value: None
Previous value: Facility (Far End)
       CLFI:
       NE: 35 EQP:STS1
       LOCATION: POS: 1
       Shelf: 1 CPG: G2 Port: 1
```

The following are examples of FAC401 INFO logs for OC-3. (Similar examples apply to OC-12.) Such logs are generated as a result of the user changing LineUAS threshold data as follows:

Threshold crossing report type: changing the present value field from “alarm” to “alert” or from “alert” to “alarm”

```
       FAC401 JUL16 11:22:49 4619 INFO Data Changed
Facility type:OC3
Parameter changed: Line Rx PM Thresh Rpt Type
Present value: Alarm
Previous value: Alert
CLFI:
       NE:22 EQP:OC3
       LOCATION: POS: 1
       Shelf: 1 CPG:G3 Port: --
```

—continued—

FAC401, continued

Threshold definition: changing the present value field to a given number and interval

```
       FAC401 JUL16 11:23:32 4720 INFO Data Changed
Facility type:OC3
Parameter changed:LineUasThresh1
Present value: 1/timed
Previous value: 13340/timed
CLFI:
       NE:22 EQP:OC3
       LOCATION: POS: 1
       Shelf: 1 CPG:G3 Port: --
```

Threshold status: changing the present value field from “enabled” to “disabled” or from “disabled” to “enabled”

```
       FAC401 JUL16 11:22:45 4518 INFO Data Changed
Facility type:OC3
Parameter changed:LineUasThresh1 Enable
Present value: Disabled
Previous value: Enabled
CLFI:
       NE:22 EQP:OC3
       LOCATION: POS: 1
       Shelf: 1 CPG:G3 Port: --
```

The following is an example of a FAC401 INFO log generated as a result of the user successfully changing the AIS threshold value.

```
       FAC401 JUL16 11:22:45 4518 INFO Data Changed
Facility type: ESI
Parameter changed: AIS Threshold
Present value: ST2
Previous value: ST1
CLFI:
       NE:33 Ottawa EQP:ESI
       LOCATION: Bay 6 POS: 1
       Shelf: 1 CPG:G1 Port: 1
```

—continued—

FAC401, continued

Field descriptions

The following table explains each of the fields in this log report.

Table 1
Log report fields

Field	Value	Description
Facility type	DS1, DS3 OC-3, OC-12, STS-1, or ESI	Type of facility that experienced the problem
Parameter changed	For DS1/DS3 LT, see Table 2 For OC3/OC12 ST, see Table 3 For ESI, see Table 4 For other parameters, see Table 5	Identifies the parameter to be changed
Present value	ASCII string	Current value of the modified parameter
Previous value	ASCII string	Previous value of the modified parameter
CLFI	ASCII string	Common language facility identifier
NE	1 to 32767	Network element identifier
EQP	DS1, DS3, OC3, OC12, STS-1, or ESI	Equipment identification
LOCATION	ASCII string	Frame name
POS	Integer value	Frame position
Shelf	Integer value	Shelf position within the frame
CPG	ASCII string	Circuit pack group identifier
Port	Integer value	Port number within the card

—continued—

FAC401, continued

DS1/DS3 LT

The following table lists examples of the parameters for a DS1/DS3 facility line termination and the corresponding STS1 path termination.

Table 2
Parameters for DS1/DS3 LT

Parameter	Parameter range
Framing Format	SF, ESF, DCL (TR-08), null
Loopback	Term (inal), Fac (ility), None
Line Build Out	Short, Long
Line CV Rx PM	T1, T2, Thresh1, Thresh2
Line ES Rx PM	T1, T2, Thresh1, Thresh2
Line SES Rx PM	T1, T2, Thresh1, Thresh2
PM threshold format	Alarm, Alert
create containment	currently not changeable
Path RX threshold format	Alarm, Alert
Path FE threshold format	Alarm, Alert
Path CV Rx PM	T1, T2, Thresh1, Thresh2
Path ES Rx PM	T1, T2, Thresh1, Thresh2
Path SES Rx PM	T1, T2, Thresh1, Thresh2
Path CV FE PM	T1, T2, Thresh1, Thresh2
Path ES FE PM	T1, T2, Thresh1, Thresh2
Path SES FE PM	T1, T2, Thresh1, Thresh2

—continued—

FAC401, continued

OC-3/OC-12 ST

The following table lists the parameters for an OC-3/OC-12 facility section termination and the corresponding STS12 section termination.

Table 3
Parameters for OC-3/OC-12 ST

Attribute type	Parameter range
Span RX threshold format	Alarm, Alert
Eqmt RX threshold format	Alarm, Alert
Eqmt RX threshold format	Alarm, Alert
Span CV Rx PM	T1, T2, Thresh1, Thresh2
Span SES Rx PM	T1, T2, Thresh1, Thresh2
Span ES Rx PM	T1, T2, Thresh1, Thresh2
Span SEFS Rx PM	T1, T2, Thresh1, Thresh2
Rx_Optics	T1, Thresh1
Rx_Optics	T1, Thresh1
Tx_LBC_p_eq	T1, Thresh1
CLFI	<ascii string>
Line RX threshold format	Alarm, Alert
Signal degrade threshold	<4 to 10>
Line CV Rx PM	T1, T2, Thresh1, Thresh2
Line ES Rx PM	T1, T2, Thresh1, Thresh2
Line SES Rx PM	T1, T2, Thresh1, Thresh2

ESI

The following table lists the parameters for an ESI facility section termination.

Table 4
Parameters for ESI

Attribute type	Parameter range
AIS Quality Lvl Threshold	Stratum 1, Stratum 2, Stratum 3, SONET Internal Clock, NULL

—continued—

FAC401, continued

Examples of other parameters that can be changed are as follows.

Table 5
Other parameters that can be changed

Parameter	Parameter range
CLFI	ASCII string
Threshold format (for example, Line Rx PM Thresh Rpt Type)	Alarm, alert
Signal degrade threshold	4 to 10
PM threshold value (for example, LineCv Thresh1)	number: 1-4,294,967,295 (varies with PM parameter) interval: timed, day, untimed
PM threshold enabled (for example, Line CVthresh1 Enable)	Enabled, Disabled
Line UAS Rx PM	T1, T2, Thresh1, Thresh2
Threshold AIS	Stratum 1, Stratum 2, Stratum 3, Sonet Clock, Null

Action

No action is required. This log is for information only.

—end—

FAC402

Report explanation

This log is generated when a termination has been created or deleted for the “ALL” selection of the circuit pack. This log report indicates that a termination has been created or deleted successfully. A FAC402 log is generated whenever a COMM SDCC (SONET data communications channels) facility is deleted or created.

Report format

The following is the format for log report FAC402.

```
FAC402 mmm:dd hh:mm:ss nnnn event_type event_label
Facility type: <type>
Operation: <operation>
CLFI: <clfi>
     NE: <ne>                         EQP: <eqp>
     LOCATION: <location>             POS: <pos>
     Shelf: <shelf>    CPG: <cpg>     Port: <port>
```

Report example

The following are examples of different types of FAC402 log reports.

```
FAC402 NOV23 21:42:23 0200 INFO Delete/Create
Operation: Delete
Facility type: DS1
CLFI:
     NE: 35                          EQP: DS1
     LOCATION:                       POS: 2
     Shelf: 1    CPG: G1             Port: 1
```

FAC402 for a DS3 Facility type:

```
       FAC402 MAR23 21:40:05 0100 INFO Delete/create
Operation: Delete
Facility type: DS3
       CLFI:
       NE:35 EQP: DS3
       LOCATION: POS: 2
       Shelf: 1 CPG: G1 Port: 1
```

—continued—

FAC402, continued

FAC402 for a STS-1 Facility type:

```
       FAC402 APR21 19:57:20 2500 INFO Delete/create
Operation: Delete
Facility type: STS1
       CLFI:
       NE:35 EQP: STS1
       LOCATION: POS: 1
       Shelf: 1 CPG: G2 Port: 3
```

FAC402 log generated when SDCC port is deleted:

```
       FAC402 FEB15 21:21:01 6600 INFO Delete/create
Operation: Delete
Facility type: COMM
       CLFI:
       NE: 25 EQP:
       LOCATION: POS:
       Shelf: 1 CPG: SDCC Port: 1
```

FAC402 log generated when an SDCC port is created:

```
       FAC402 FEB 17 11:43:20 8500 INFO Delete/create
Operation: Create
Facility type: COMM
       CLFI:
       NE: 25 EQP:
       LOCATION: POS:
       Shelf: 1 CPG: SDCC Port: 1
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<type>	DS1, DS3, OC-3, OC-12, STS-1, or COMM	Type of facility that experienced the problem
<operation>	Add, Delete	Type of provisioning operation
<clfi>	ASCII string	Common language facility identifier
<ne>	1 to 32767	Network element identifier
<eqp>	DS1, DS3, OC-3, OC-12, or STS-1	Equipment type
—continued—		

FAC402, continued

Field	Value	Description
<location>	ASCII string	Frame name
<pos>	Integer value	Frame position
<shelf>	Integer value	Shelf position within the frame
<cpg>	ASCII string	Card position within the shelf
<port>	Integer value	Port number within the card
	—end—	

Action

No action is required. This log is for information only.

—end—

FAC403

Report explanation

This log reports the number of DS1, DS3, or STS-1 ports created on autoprovisioning for a DS1, DS3, or STS-1 circuit pack group.

Report format

The following is the format for log report FAC403.

```
FAC403 mmm:dd hh:mm:ss nnnn event_type event_label
Facility type: <type>
     NE: <ne>                               EQP: <eqp>
     LOCATION: <location>                   POS: <pos>
     Shelf: <shelf>      CPG: <cpg>         Ports created: <ports>
```

Report example

The following shows a typical example of log report FAC403.

```
FAC403 MAR23 21:42:23 0200 INFO Create
Facility type: DS1
     NE: 35                                 EQP: DS1
     LOCATION:                              POS: 2
     Shelf: 1        CPG: G1                Ports created: 14
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<type>	DS1, DS3, or STS-1	Type of facility
<ne>	integer	Network element
<eqp>	DS1, DS3, or STS-1	Equipment type
<location>	Alphanumeric	Frame name
<pos>	numeric	Frame position
<shelf>	numeric	Shelf position within the frame
<cpg>	Alphanumeric	Card position within the shelf

—continued—

—continued—

FAC403, continued

Field	Value	Description
<ports>	integer (1 to 14)	Number of new ports created during autoprovisioning for the circuit packgroup.
	—end—	

Action

None

—end—

FAC404

Report explanation

This log report describes an add/drop or pass through on a network element. A FAC404 log is generated whenever an STS or VT connection is created or deleted. Transport optics end point can be G1 or G1S/G2. Tributary ends can be DS1, DS3, STS-1, or OC-3.

Report example

STS-1 connection

The following are examples of different types of FAC404 log reports for STS-1 connections.

FAC404 log for the creation of a pass through connection on an STS-1 channel 1 from transport optics G1 to G1S/G2:

```
      FAC404 OCT27 14:33:37 8600 INFO Connection Services
Operation:Create                   Rate:STS-1
Connection:Channel #1 on G1 to Channel #1 on G1S/G2
      NE:32 Ottawa
      LOCATION: Bay 6    POS: 1
      Shelf: 1
```

FAC404 log for the deletion of a pass through connection on STS-1 channel 2 from transport optics G1 to G1S/G2:

```
      FAC404 OCT27 14:33:05 8500 INFO Connection Services
Operation:Delete                   Rate:STS-1
Connection:Channel #2 on G1 to Channel #2 on G1S/G2
      NE:32 Ottawa
      LOCATION: Bay 6    POS: 1
      Shelf:1
```

—continued—

FAC404, continued

FAC404 log for the creation of an add/drop connection on STS-1 channel 4 from G1 to tributary STS1 G1 port 1:

```
      FAC404 OCT27 14:36:32 8700 INFO Connection Services
Operation:Create                   Rate:STS-1
Connection: Channel #4 on G1 to STS-1 G1 Port #1
      NE:32 Ottawa
      LOCATION: Bay 6    POS: 1
      Shelf:1
```

FAC404 for the setup of a transport VT-managed STS-1 port:

```
      FAC404 OCT17 18:10:49 5400 INFO Connection Services
Operation:Create                   Rate:STS-1
Connection: Channel #4 on G1 to VT-managed
      NE:41 Ottawa
      LOCATION: Bay 6    POS: 1
      Shelf: 1
```

The following is an example of an FAC404 log report for an STS-3c connection.

FAC404 for the creation of an STS-3c channel 4 add/drop connection from G1 to tributary OC3, G3, port 1:

```
      FAC404 OCT17 18:10:49 5400 INFO Connection Services
Operation:Create                   Rate:STS-3c
Connection: Channel #4 on G1 to OC3 G3 Port #1
      NE:41 Ottawa
      LOCATION: Bay 6    POS: 1
      Shelf: 1
```

FAC404 for the creation of a pre-provisioned STS-3c channel 4 add/drop connection from G1 to port 1 OC3 G3 with no tributary provisioned in slot 15, port 1:

```
      FAC404 OCT17 18:10:49 5400 INFO Connection Services
Operation:Create                   Rate:STS-3c
Connection: Channel #4 on G1 to OC3 G3 Slot 15 Port #1
      NE:41 Ottawa
      LOCATION: Bay 6    POS: 1
      Shelf: 1
```

—continued—

FAC404, continued

VT1.5 connection

The following are examples of different types of FAC404 log reports for VT1.5 connections.

FAC404 log for the creation of a pass through connection on STS-1 channel 4 from transport optics G1 to G1S/G2:

```
      FAC404 OCT27 14:33:05 8500 INFO Connection Services
Operation:Create                   Rate:VT1.5
Connection:Channel #4,1,1 on G1 to Channel #4,1,1 on G1S/G2
      NE:42 Ottawa
      LOCATION: Bay 6    POS: 1
      Shelf:1
```

Field descriptions

Field	Value	Description
Operation	Create, delete	Type of operation performed
Rate	STS-1, STS-3c, VT1.5	Rate of connection
Connection	Internal end points of connection	Internal connectivity on the NE between the transport optics and either a tributary or another set of transport optics
NE	1 to 32767	Network element identifier
LOCATION	ASCII string	Frame name
POS	Integer value	Frame position
Shelf	Integer value	Shelf position within the frame

Action

No action is required. This log is for information only.

—end—

FAC405

Report explanation

This log reports that an edit to Timing Reference Operation has been successful completed. Operations such as ‘Edit Primary or Secondary timing reference’ will generate this log.

Report format

The following is the format for log report FAC405.

```
FAC405 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: <object class>
Parameter changed: <parameter>
Present value: <present>
Previous value: <previous>
     NE: <ne>                             EQP: <eqp>
     LOCATION: <location>                 POS: <pos>
     Shelf: <shelf>      CPG: <cpg>       Port: <port>
     Protectn Gp: <protection group>      Member: <member>
```

Report example

The following shows a typical example of log report FAC405.

```
FAC405 NOV23 21:42:23 0200 INFO Data Changed
Object Class: Redundancy Group Member
Parameter changed: Source Selection
Present value: NULL
Previous value: BITSB
     NE: 100                         EQP: ES1
     LOCATION:                       POS: 1
     Shelf: 1        CPG: G1         Port: 14
     Protectn Gp: 12                 Member: TimGen Pri
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<object class>	Redundancy Group Member	Type of facility being changed
<parameter>	Source Selection	Parameter being changed

—continued—

—continued—

FAC405, continued

Field	Value	Description
<present>	BITS, BITSB, OCA, OCB, NULL	Present value of the parameter being changed
<previous>	BITS, BITSB, OCA, OCB, NULL	Previous value of the parameter being changed
<ne>	integer	Network element
<eqp>	DS1 or DS3	Equipment type
<location>	Alphanumeric	Frame name
<pos>	numeric	Frame position
<shelf>	numeric	Shelf position within the frame
<cpg>	Alphanumeric	Card position within the shelf
<protection group>	12	Protection group number
<member>	TimGen Pri, TimGen Sec	Primary or secondary timing reference
—end—		

Action

None is required; log is for information purposes only.

—end—

FAC406

Report explanation

This log report indicates that the quality level of a timing reference has been successfully changed. This attribute is changed using the timing reference protection screen.

Report example

The following is an example of a FAC406 INFO log generated as a result of the user successfully changing the quality level of the timing reference.

```
      FAC406 JUL16 11:22:45 4518 INFO Data Changed
Object class: Timing Source
Parameter changed: Quality Level
Present value: S2-F
Previous value: S1
      NE: 634            EQP: TGen
      LOCATION: TOWER5   POS: 1
      Shelf: 1           Src: OC12 G1
      PROTECTN GRP: 31   MEMBER: 1
```

—continued—

FAC406, continued

Field descriptions

Field	Value	Description
Object class	Timing Source	Object being changed
Parameter changed	Quality Level	Identifies the parameter to be changed.
Present value	ST1, STU, ST2, ST3, SIC, DUS, RES, Auto	Current quality level of the timing reference
Previous value	ST1, STU, ST2, ST3, SIC, DUS, RES, Auto	Previous quality level of the timing reference
NE	1 to 32767	Network element identifier
EQP	TGen	Equipment identification
LOCATION	ASCII string	Frame name
POS	Integer value	Frame position
Shelf	Integer value	Shelf position within the frame
Src	OC12 G1, OC12 G2, BITSA, BITSB	Source of the timing reference
PROTECTN GRP	Integer value	Protection group number
MEMBER	Integer value	Identifier of a protection group member

Action

No action is required. This log is for information only.

—end—

FAC407

Report explanation

This log report indicates a timing reference has been provisioned or deprovisioned in the timing reference protection screen.

Report example

The following is an example of a FAC407 INFO log generated as a result of the user provisioning a timing reference.

```
      FAC407 JUL16 11:22:45 4518 INFO Data Changed
Operation: Create
Object class: Protection Unit
      NE: 634             EQP: TGen
      LOCATION: TOWER5    POS: 1
      Shelf: 1            Src: OC12 G1
      PROTECTN GRP: 31    MEMBER: 1
```

Field descriptions

Field	Value	Description
Operation	Create, Delete	Type of provisioning operation
Object class	Protection Unit	Object being changed
NE	1 to 32767	Network element identifier
EQP	TGen	Equipment identification
LOCATION	ASCII string	Frame name
POS	Integer value	Frame position
Shelf	Integer value	Shelf position within the frame
Src	OC12, G1, OC12 G2, BITSA, BITSB	Source of the timing reference
PROTECTN GRP	Integer value	Protection group number
MEMBER	Integer value	Identifier of a protection group member

Action

No action is required. This log is for information only.

—end—

FAC501

Report explanation

This log report indicates that a manual state change has been invoked. State transitions from the following do not generate logs.

- IS_NR to IS_ANR
- IS_ANR to IS_NR
- OOS_MT to OOS_MA
- OOS_MA to OOS_MT

Note: Taking the OC-12 facilities out of service on a regenerator shelf does not generate this log.

Report format

The following is the format for log report FAC501.

```
FAC501 mmm:dd hh:mm:ss nnnn event_type event_label
Facility type: <type>
Present state: <pres state>
Previous state: <prev state>
CLFI: <clfi>
     NE: <ne>                          EQP: <eqp>
     LOCATION: <location>              POS: <pos>
     Shelf: <shelf>     CPG: <cpg>     Port: <port>
```

Report example

The following are examples of a FAC501 log report for DS3, STS-1, and OC-12 Facility types:

```
       FAC501 MAR23 21:45:49 0300 INFO State Change
Facility type: DS3
Present state: OOS MTC
Previous state: IS TRBL
       CLFI: PAUL
       NE:35 EQP: DS3
       LOCATION: POS: 2
       Shelf: 1 CPG: G1 Port: 2
```

—continued—

FAC501, continued

```
       FAC501 APR21 19:57:57 3300 INFO State Change
Facility type: STS1
Present state: IS TRBL
Previous state: OOS
       CLFI:
       NE:35 EQP: STS1
       LOCATION: POS: 1
       Shelf: 1 CPG: G2 Port: 3

FAC501 NOV23 21:45:49 0300 INFO State Change
Facility type: OC12
Present state: IS
Previous state: OOS
CLFI:
     NE: 12 Main St                  EQP: OC12
     LOCATION: TORONTO               POS: 1
     Shelf: 1        CPG: G1S        Port: 2
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<type>	DS1, DS3, OC-3, OC-12, or STS-1	Type of facility which experienced the problem
<pres state>	IS, OOS, IS TRBL, OOS MTC	Current state of facility
<prev state>	IS, OOS, IS TRBL, OOS MTC	Previous state of facility
<clfi>	alphanumeric	Common language facility identifier
<ne>	1 to 32767	Network element
<eqp>	DS1, DS3, OC-3, OC-12, or STS-1	Equipment type
<location>	alphanumeric	Frame name
<pos>	numeric	Frame position
<shelf>	numeric	Shelf position within the frame
<cpg>	alphanumeric	Circuit card position within the shelf
<port>	integer	Port number within the card

—continued—

FAC501, continued

Action

No action is required. This log is for information only.

—end—

FAC502

Report explanation

This log reports the number of DS1, DS3, or STS-1 ports that had a state change during autoprovisioning for the specified DS1, DS3, or STS-1 group.

Report format

The following is the format for log report FAC502.

```
FAC502 mmm:dd hh:mm:ss nnnn event_type event_label
Facility type: <type>
Present state: <pres state>
Previous state: <prev state>
CLFI: <clfi>
     NE: <ne>                              EQP: <eqp>
     LOCATION: <location>                  POS: <pos>
     Shelf: <shelf>       CPG: <cpg>       Ports affected: <ports>
```

Report example

The following shows a typical example of log report FAC502.

```
FAC502 nov23 21:45:49 0300 INFO State Change
Facility type: DS1
Present state: OOS
Previous state: IS
CLFI:
     NE: 35                          EQP: DS1
     LOCATION:                       POS: 2
     Shelf: 1         CPG: G1        Ports affected: 14
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<type>	DS1, DS3, or STS-1	The type of facility
<pres state>	IS or OOS	Present state of facility: In service (IS) or Out of service (OOS)
<prev state>	IS or OOS	Previous state of facility: In service (IS) or Out of service (OOS)

—continued—

—continued—

FAC502, continued

Field	Value	Description
<clfi>	alphanumeric	Common language facility identifier
<ne>	integer	Network element
<eqp>	DS1, DS3, or STS-1	Equipment type
<location>	alphanumeric	The frame name
<pos>	numeric	Frame position
<shelf>	numeric	Shelf position within the frame
<cpg>	alphanumeric	Card position within the shelf
<ports>	integer	Number of ports within the circuit pack group that experienced a state change

—end—

Action

None

—end—

FAC601

Report explanation

This log is generated when a performance monitoring (PM) operation is successful.

The following are examples of a performance monitoring operation that will generate this log.

1 When PM counts are reset.

2 When an untimed interval has been successfully started.

Report format

The following is the format for log report FAC601.

```
FAC601 mmm:dd hh:mm:ss nnnn event_type event_label
Facility type: <type>
Operation: <operation>
CLFI: <clfi>
     NE: <ne>                        EQP: <eqp>
     LOCATION: <location>            POS: <pos>
     Shelf: <shelf>  CPG: <cpg>      Port: <port>
```

Report example

The following shows a typical example of log report FAC601.

```
FAC601 MAR23 22:26:08 1400 INFO PM operation
Facility type: DS1
Operation: Start Untimed Interval
CLFI:
     NE: 35                          EQP: DS1
     LOCATION:                       POS: 2
     Shelf: 1        CPG: G1         Port: 2
```

—continued—

FAC601, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<type>	DS1, DS3, STS-1, OC-3, OC-12	Type of facility
<operation>	Start Untimed Interval Clear HISTORY and CURRENT Clear HISTORY Clear CURRENT	PM operation performed
<clfi>	alphanumeric	Common language facility identifier
<ne>	integer	Network element
<eqp>	DS1, DS3, STS-1, OC-3, OC-12	Equipment type
<location>	alphanumeric	Frame name
<pos>	numeric	Frame position
<shelf>	numeric	Shelf position within the frame
<cpg>	alphanumeric	Card position within the shelf
<port>	integer	Port number within the card

Action

None

—end—

FAC605

Report explanation

This log report indicates that a timing reference protection switch has occurred.

Report example

The following is an example of a FAC605 log report for a timing reference protection switch:

```
      FAC605 NOV24 13:57:58 2300 Protection activity
Object Class: Synchronization Manager
Operation: Pre-empt
Reason: Auto (Local)
      NE: 20            EQP: TGen
      LOCATION:         POS: 1
      Shelf: 1          Src: OC12 G1
      PROTECTN GRP: 99   MEMBER: 1
```

—continued—

FAC605, continued

Field descriptions

Field	Value	Description
Object Class	Synchronization Manager	Class of the object
Operation	Operate Release Pre-empt	Operation performed
Reason	Auto (Local) Auto (Remote) Force (Local) Force (Remote) Manual (Local) Manual (Remote) Signal/Eqp Fail (Local) Signal/Eqp Fail (Remote) Signal Degrade (Local) Signal Degrade (Remote)	Protection operation that was performed, released, or preempted
NE	1 to 32767	Network element identifier
EQP	TGen	Equipment identification
LOCATION	ASCII string	Frame name
POS	Integer value	Frame position
Shelf	Integer value	Shelf position within the frame
Src	OC12G1, OC12 G2, BITSA, BITSB	Source of the timing reference
PROTECTN GRP	Integer value	Protection group number
MEMBER	Integer value	Identifier of a protection group member

Action

No action is required. This log is for information only.

—end—

FAC606

Report explanation

A protection activity was performed or released successfully, or was pre-empted due to a higher priority activity, or went into a wait-to-restore period upon release.

Report format

The following is the format for log report FAC606.

FACP606 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: <class>
Operation: <operation>
Reason: <reason>

Report example

The following shows a typical example of log report FAC606.

```
FAC606 NOV26 14:16:06 1800 INFO Protection Activity
Object Class: Redundancy Group Member
Operation: Operate
Reason: Manual (Local)
     NE: 661             EQP: AccessNode
     LOCATION: 1         POS: 1
     SHELF: 1            CPG:--PORT:
     PROTECTN GRP:       MEMBER: DS1 G1
```

—continued—

FAC606, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<class>	text string	String identifying the object class that failed/denied the protection request.
<operation>	Operate Release Preempt	Protection operation performed.
<reason>	Auto (Local) Auto (Remote) Force (Local) Force (Remote) Lockout (Local) Lockout (Remote) Manual (Local) Manual (Remote) Signal/Eqp Fail (Local) Signal/Eqp Fail (Remote) Signal Degrade (Local) Signal Degrade (Remote) STS1 PathOverhead switch Wait to restore (Local) Wait to restore (Remote)	Type of protection operation that was performed, released or pre-empted. Note: an STS1 PathOverhead switch will only generate this log when performed (not upon a release).

Action

None

—end—

FAC607

Report explanation

This log indicates a DS1 VT misconnection, a VT passthru misconnection or a STS-1 VT misconnection.

This log report indicates that a misconnection has occurred as a result of the provisioning of a VT1.5 connection as follows:

- a VT1.5 add-drop connection of a DS1/STS-1/OC-3 is provisioned using the transport STS-1 channel allocated for VT1.5 connections of another STS-1/OC-3 port
- a VT1.5 add-drop connection of a STS-1/OC-3 is provisioned with the VT group and VT number mismatched with the transport STS-1 VT group and VT number
- a VT1.5 pass-through connection is provisioned using the transport STS-1 channel allocated for VT1.5 connections of an STS-1/OC-3 port

Report format

The following is the format for log report FAC607.

FACP607 mmm:dd hh:mm:ss nnnn event_type event_label
Object Class: <class>
Operation: <operation>
Reason: <reason>

Report example

The following are typical examples of log report FAC607.

```
FAC607 JUL21 14:10:21 5200 INFO Misconnection found
Event:Misconnection found on VT connection provisioning
Origination:Tributary DS1 G9 Port 2
Termination:Transport Channel #1,1,3 on G1
NE:649
LOCATION: 1          POS: 1
Shelf: 1
```

—continued—

FAC607, continued

```
       FAC607 JUL21 14:18:59 5500 INFO Misconnection found
Event: Misconnection found on VT connection provisioning
Origination: Transport Channel #1, 1, 4 on G1
Termination: Transport Channel #1, 1, 4 on G1S/G2
       NE: 649
       LOCATION: 1 POS: 1
       Shelf: 1

       FAC607 JUL21 14:20:51 5700 INFO Misconnection found
Event: Misconnection found on VT connection provisioning
Origination: Transport Channel #1, 1, 2 on G1S/G2
Termination: Tributary STS1 G2 Port #1, 1, 2
       NE: 649
       LOCATION: 1 POS: 1
       Shelf: 1
```

Field descriptions

Field	**Value**	**Description**
Event	ASCII string	Type of event reported
Origination	Internal end point of connection	Origination of the VT1.5 connection: either a transport port or a tributary port
Termination	Internal end point of connection	Termination of the VT1.5 connection: either a transport port or a tributary port
NE	1 to 32767	Network element identifier
Location	ASCII string	Frame name
POS	Integer value	Frame position
Shelf	Integer value	Shelf position within the frame

Action

Step	**Action**
1	Remove the VT1.5 connection as indicated or investigate the misuse of the transport STS-1 channel for the VT1.5 connection provisioning.

—end—

FAC608

Report explanation

This log indicates the success of path protection switch (PPS).

Report format

The following is the format for log report FAC608.

```
FACP608
HostName: <host name>
Active Port: <active port>
LinkType: <link type>
```

Action

None

—end—

FAC609

Report explanation

This log indicates the failure of path protection switch (PPS).

Report format

The following is the format for log report FAC609.

```
FACP609
HostName: <host name>
Active Port: <active port>
LinkType: <link type>
```

Action

None

—end—

FLT700

Report explanation

This log report is generated to provide Nortel Networks support personnel with additional information about a TIC, LIC, AIC, CDSP, MIC, TAC, Proc, IRTU, OC-3, OC-12, ESI, DS1, DS3, STS-1, and TXC circuit pack group alarm. Fault strings in this log, map directly to circuit pack alarms, except for “unequipped” and “mismatch” circuit pack alarms.

Report format

The following is the format for log report FLT700.

FLT700 mmm:dd hh:mm:ss nnnn event_type event_label
Location fields.
Fault: <fault id> <fault string>

Report example

The following shows a typical example of log report FLT700.

```
FLT700 MAY12 12:34:56 1234 INFO Equipment Fault
NE: 162              LOCATION: 1
EQP: 1 ABM FCOT
SHELF POS: 1         SHELF: CDS 1
CPG: NLIC D          SLOT: 97
FAULT: 88 Card Access Failure
```

Field descriptions

The following table shows the values for the fault field in this log report.

Field	Value	Description
<fault id>	numeric character	Fault identifier
<fault string>	text string	Fault string that appears for the circuit pack identified in the location fields

Action

The information in this log is used by Nortel Networks repair personnel to assist in diagnosing circuit pack faults. Forward a copy of this log along with any failed circuit packs to your Nortel Networks repair center.

Refer to the AccessNode Technical Support Reference Card for the address and phone number of the US and Canadian repair centers.

—end—

FWDB300

Report explanation

The database backup was unsuccessful. This can happen if the OPC is down, if one of the NEs on the path to the OPC is down, or if there are communication problems along the way (check for communication logs).

Report format

The following is the format for the FWDB300 log report.

FWDB300 mmm:dd hh:mm:ss nnnn event_type event_label
Destination: <destination>
Status: <status>   Attempts Made: <attempts>

Report example

The following shows a typical example of the FWDB300 log report.

```
FWDB300 MAY01 01:51:38 4100 INFO DB Backup
Status: No Response    Attempts Made: 3
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<destination>	MATE or OPC	Destination for the backup database
<status>	No Response Failed	The result of the database operation: – if destination OPC – if destination MATE
<attempts>	integer	Number of operation attempts made.

Action

Identify the source of the problem. Check for OPC equipment alarms that may indicate a problem with the OPC. The database backup will automatically be reattempted every 24 hours (or as scheduled). The operator can also perform a manual backup when the problem is identified and resolved. To perform a manual database backup, refer to *Data Administration Procedures*, 323-3001-304 in *Operations, Administration, and Provisioning,* Volume 4A.

If the destination for the backup is the MATE, the backup operation is automatically reattempted if the state of the inactive is IS_NR and communication between processors is functioning. If this fault persists, look for these related processor equipment alarms and proceed accordingly:
– Loss of mate communication
– Loss of duplex
– Loss of datasync

—end—

FWDB301

Report explanation

Restoration of the database was unsuccessful.

Report format

The following is the format for the FWDB301 log report.

```
FWDB301 mmm:dd hh:mm:ss
Source: <source>
Status: <status>            Attempts Made: <attempts>
Elapsed Time: <time>        Generation: <gen>
```

Report example

The following is a typical example of the FWDB301 log report.

```
FWDB301 MAY01 01:51:38 4100 INFO DB Restore
Source: OPC
Status: No Response    Attempts Made: 3
Generation: Current
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<source>	MATE or OPC	Source of the database for the restoration
<status>		The result of the database operation:
(for OPC source)	No Response	– OPC not communicating. Will use what's in RAM.
	Audit Failed	– An application written audit procedure failed.
	Checksum Failed	– Corrupt DB backup
	Los Prov. Data	– There may be loss of provisioning data.
	No Backups	– No database backups are found at the OPC.
(for MATE source)	Audit Failed	– An application written audit procedure failed.
<attempts>	integer	Number of operation attempts made
<gen>		
(for OPC source)	Current	– latest backup to the OPC
	Backup1	– prior backup to the OPC
(for MATE source)		Not applicable

—continued—

FWDB301, continued

Action

The action to be performed depends on the value of the status field:

- If the status is No Response, the OPC is down, or there is a communication failure on an NE on the path to the OPC, or at the OPC itself. When the problem is identified and solved, the restore function will be performed. Until then, the UI and OAM functions at the NE are not operational.
- If the status is Audit Failed, the software, which verifies the sanity of a restore database, has detected an error. This can occur for one of two reasons:
  - — The database is corrupted at the OPC.
  - — There is a software error at the NE.

In either case, the Backup and Restore Manager attempts a restore using the previous backup file. If this also fails, the database is cleared and an “empty” database is used (the database created by the autoprovisioning process). The operator should check for a SWERR log to see if any audit procedures reported a software error, and send these to Nortel Networks.

- If the status is Checksum Failed, the Backup and Restore Manager has restored a corrupted database and automatically attempts to restore the previous backup. If this also fails, the database is cleared and an “empty” database is used. The operator should investigate the operation of the OPC to see why the backup file became corrupted.
- If the status is Lost Prov. Data, the Backup and Restore Manager has detected that the database restored from the OPC was not complete. It detects this by comparing a “checkpoint” value stored at the OPC with that in the NE’s nonvolatile storage. If they do not match, provisioning data may have been lost. The operator should verify that the last provisioning changes are present at the NE.
- If the status is No backup, the backup files for the NE were lost or deleted at the OPC, unless this NE was being brought up for the first time. The NE is initialized with an “empty” database.

—end—

FWDB400

Report explanation

The database backup was successful.

Report format

The following is the format for the FWDB400 log report.

FWDB400 mmm:dd hh:mm:ss nnnn event_type event_label

DESTINATION: <destination>
Status: <status> Attempts Made: <attempts>
Elapsed Time: <eltime>

Report example

The following shows a typical example of the FWDB400 log report.

```
FWDB400 MAY01 01:51:38 4100 INFO DB Backup
Destination:  OPC
Status: Complete         Attempts Made: 1
Elapsed Time: 00:00:11.080
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
DESTINATION	OPC Mate	Backup going to OPC or Mate processor
<status>		The result of the database operation:
	Completed	– Successful database backup to the OPC
<attempts>	integer	Number of operation attempts made
<elapsed time>	hh:mm:ss. msec	Time it took to perform the backup

Action

None

—end—

FWDB401

Report explanation

The database restore was successful.

Report format

The following is the format for the FWDB401 log report.

```
FWDB401 mmm:dd hh:mm:ss nnnn event_type event_label
Source: <source>
Status: <status>              Attempts Made: <attempts>
Elapsed Time: <eltime>        Generation: <gen>
```

Report example

The following shows a typical example of the FWDB401 log report.

```
FWDB401 MAY01 01:51:38 4100 INFO DB Restore
Source: OPC
Status: Complete             Attempts Made: 1
Elapsed Time: 00:00:11.080   Generation: Current
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<source>	OPC	Restore was from OPC
	RAM	Restore was from RAM
	MATE	Restore was from the mate
<status>		The result of the database operation: – Successful database backup to the OPC
	Completed	
<attempts>	integer	Number of operation attempts made
<eltime>	hh:mm:ss. msec	The time it took to perform the backup
<gen>	Current	– latest backup to the OPC
	Backup1	– prior backup to the OPC
	RAM	– latest backup version in RAM
	< >	– Restore from RAM or mate: Generation n/a here

Action

None

—end—

FWDB402

Report explanation

The OPC was unavailable so the database was restored from random access memory (RAM).

Report format

The following is the format for the FWDB402 log report.

FWDB402 mmm:dd hh:mm:ss nnnn event_type event_label
OPC Unavailable
Database Restored from RAM

Report example

The following shows a typical example of the FWDB402 log report.

```
FWDB402 MAY01 01:51:38 4100 INFO DB Restore
OPC Unavailable
Database Restored from RAM
```

Action

None

—end—

FWDB403

Report explanation

This log report indicates that the processor synchronization state has changed. The log only appears on dual-processor configurations.

Report example

The following shows a typical example of the FWDB403 log report.

```
CM     FWDB403 DEC01 19:21:38 6200 INFO DB Sync
Processor Synchronization:  Disabled
```

Field descriptions

The following table gives the field descriptions for this log report.

Field	Value	Description
<processor synchronization>	Disabled	The dual-processor state is disabled.
	Enables	The dual-processor state is enabled.

Action

None. This log is informational only.

—end—

GEN300

Report explanation

This log report indicates is generated when an NE informs the OPC that it was forced to discard log information.

Report severity

Warning

Report format

The following is the format for a GEN300 log report.

GEN300 NE <ne name> <ne id> has lost <number> logs.

Report example

The following is a typical example of a GEN300 log report.

```
GEN300 NE Chicago2 3234 has lost 20 logs.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<NE name>	Character string	The name of the NE which lost the logs
<ne ID>	Decimal	The id of the NE which lost the logs

Action

Check the Alarm Monitor and Event Browser for alarms and logs being stored by the OPC and solve accordingly. If there is no unusual problems, check the logs that the network element is generating (using logutil). Again, if no unusual problems are occurring, contact Nortel Networks support.

—end—

GEN302

Report explanation

This log report indicates that insufficient memory was available to perform a requested operation.

Report severity

Major

Report format

The following is the format for a GEN302 log report:

GEN302 Not enough memory. Too many processes may be running. Close any windows you do not need, then try again.

Action

There are several limitations to the number of OPC tools which can be in use at one time. In addition to the absolute maximums defined by the system, as given below, memory limitations may prevent a tool from opening. This log is generated to record the event.

Normally, the closure of an open user interface window or the logout of another user will release sufficient memory to allow the requested operation to complete.

If this log appears often, it indicates a possible memory management problem. The conditions of operation and the frequency of the log's appearance should be reported to the Nortel Networks service representative.

The maximum number of users that can be logged into an OPC at any one time is three.

The maximum number of tools which can be opened at any one time on an OPC, depends on the type of tools which are already open, and on other activity in the OPC. This number is significantly less that the number of tools which could theoretically be opened by three users, each of whom have 15 tools open.

Maximum instances of tool types

The number of instances of a tool which are permitted to be opened within a single user session depends on the tool type. In addition, each tool type has an overall maximum number of instances which may be open on an OPC. The following table provides these limits.

—continued—

GEN302, continued

	Maximum instances per OPC			Maximum instances per user session
Tool name	**X**	**CMT**	**Total**	**X or CMT**
Alarm monitor or Network browser	3	3	6	1
Event browser	9	9	18	3
Network browser	3	3	6	1
NE login manager	3	3	6	1
Network element login	12	12	12	12
Commissioning manager	1	1	1	1
Password update	3	3	6	1
Unix shell	9	9	9	5
Centralized security manager (Group and user setup tool)	1	1	2	1
OPC save and restore	1	1	2	1
Reboot/load manager	1	1	2	1
OPC date or Shutdown	1	1	2	1
Backup and restore	1	1	2	1
Status tool	3	3	6	1
Message alarm (training demo)	1	1	2	1

—end—

GEN359

Report explanation

This log report indicates a network element commissioning error.

Report severity

Major

Report format

The following is the format for a GEN359 log report.

GEN359 Inconsistent commissioning data detected for NE <equipment identifier>. Retry commissioning of NE.

Report example

The following is a typical example of a GEN359 log report.

```
GEN359 Inconsistent commissioning data detected for NE 43. Retry
commissioning of NE.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<equipment identifier>	Decimal number	Serial number of the network element

Action

Decommission the network element defined in the log, by following the procedure in *Commissioning and Testing*, Volume 3. Then, recommission the network element by executing the commissioning procedures in the same document.

—end—

GEN360

Report explanation

This log report indicates a network element commissioning error.

Report severity

Major

Report format

The following is the format for a GEN360 log report.

GEN360 Inconsistent commissioning data detected for NE <equipment identifier>. Retry commissioning of NE.

Report example

The following is a typical example of a GEN360 log report.

```
GEN360 Inconsistent commissioning data detected for NE 43. Retry
commissioning of NE.
```

Field descriptions

The following table explains the variable field in the log report.

Field	**Value**	**Description**
<equipment identifier>	Decimal number	Serial number of the network element

Action

Decommission the network element defined in the log, by following the appropriate commissioning procedure in *Commissioning and Testing*, Volume 3. Then, recommission the network element by executing the commissioning procedures in the same document.

—end—

GEN361

Report explanation

This log report indicates a network commissioning error.

Report severity

Major

Report format

The following is the format for a GEN361 log report.

GEN361 Inconsistent network commissioning data detected. Retry commissioning of system.

Report example

The following is an example of GEN361 log report.

```
GEN361 Inconsistent network commissioning data detected. Retry
commissioning of system.
```

Action

Execute the procedure “Clearing commissioning data from a primary or backup OPC”, in *Commissioning Procedures*, 323-3001-220 in *Commissioning and Testing*, Volume 3. Then execute the procedures identified in the task “Commissioning a new span of control”, found at the beginning of the same document.

—end—

GEN362

Report explanation

This log report indicates that a network element cannot establish a communications link with the OPC. This report appears when a network element tries to establish a link with the wrong OPC or when it tries to establish a link while it is already communicating with the correct OPC.

Report severity

Major

Report format

The following is the format for a GEN362 log report.

GEN362 Inconsistent system commissioning data detected. Edit system commissioning data.

Action

Log in to the active OPC as the slat user, open the commissioning manager tool, and select the Edit System Data button. Examine the contents of the dialog which appears, and modify the contents which you find to be incorrect, by following the appropriate steps in the procedure “Entering system-level data” in *Commissioning and Testing*, Volume 3. Then execute the procedure “Transferring data from the primary to the backup OPC” in the same document.

If you cannot locate any incorrect data, execute the procedure “Clearing commissioning data from the primary or backup OPC” in *Commissioning and Testing*, Volume 3. Then execute the procedures identified in the task “Commissioning a new span of control.”

—end—

GEN363

Report explanation

This log report indicates a system commissioning error.

Report severity

Major

Report format

The following is the format for a GEN363 log report.

GEN363 Inconsistent NCF commissioning data detected. Edit system commissioning data.

Action

Log in to the active OPC as the slat user, open the commissioning manager tool, and select the Edit System Data button. Examine the contents of the dialog which appears, and modify the contents which you find to be incorrect, by following the appropriate steps in the procedure “Entering system-level data” in *Commissioning and Testing*, Volume 3. Then execute the procedure “Transferring data from the primary to the backup OPC” in the same document.

If you cannot locate any incorrect data, execute the procedure “Clearing commissioning data from the primary or backup OPC” *Commissioning and Testing*, Volume 3. Then execute the procedures identified in the task “Commissioning a new span of control”, found at the beginning of the same document.

—end—

GEN371

Report explanation

This log report indicates that the specified help file cannot be found. No on-line help is available for the associated tool.

Report severity

Minor

Report format

The following is the format for a GEN371 log report.

GEN371 File <file identifier> cannot be found.

Report example

The following shows a typical example of a GEN371 log report.

```
GEN371 File /iws/lmrhelp.text cannot be found.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<file identifier>	Text	Name of a help file

Action

Contact your Nortel Networks service representative to provide the file name given in the log report.

—end—

GEN382

Report explanation

This log report indicates that the OPC alarm database is full. The oldest alarms of lowest severity have been deleted to make room for recently arrived alarms of higher severity. Loss of alarm entries in this database does not affect current alarm counts displayed in the alarm summary line of the terminal interface screens. Low-severity alarms, which are still active when space becomes available in the database, are recovered by audits of the network elements.

Report severity

Warning

Report format

The following is the format for a GEN382 log report.

```
GEN382 Active alarms are getting lost; database is full.
```

Action

None

—end—

GEN605

Explanation

Log report GEN605 indicates that an OPC alarm has been manually cleared from the OPC Alarm Provisioning tool.

Report severity

Warning

Report format

The following is the format for a GEN605 log report:

GEN605 OPC alarm <alarm> has been manually cleared.

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<alarm>	Text	The name of the cleared OPC alarm

Action

No action is required. This log report is for information only. You can see it in the Event Browser.

—end—

GEN618

Report explanation

This log report indicates that a network element cannot establish a communications link with the OPC. This report appears when a network element tries to establish a link with the wrong OPC or when it tries to establish a link while it is already communicating the correct OPC.

Report severity

Major

Report format

The following is the format for a GEN618 log report.

GEN618 Log/Alarm database updated for NE <equipment identifier>.

Report example

The following is a typical example of a GEN618 log report.

```
GEN618 Log/Alarm database updated for NE 43.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<equipment identifier>	Decimal number	Serial number of the network element

Action

None

—end—

GEN750

Report explanation

This log report is generated several times during an incremental software delivery (ISD). Its only purpose is to provide information about the major events caused by ISD.

Report severity

Warning

Report format

The following is the format for a GEN750 log report.

GEN750 ISD: <log text>.

Report example

The following is a typical example of a GEN750 log report.

```
GEN750 ISD:Comms server must be run from ISD!
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<log text>	text	Any major event that takes place during the execution of an incremental software delivery.

Action

None

—end—

HMU311

Report explanation

This log is generated when the HMU detects an error with path protection switch (PPS) tasks. Listed below are the four types of errors that could occur.

- From the far-end, PPS receives a message larger that 256 bytes.
- PPS receives a PPS switch request on a given path type.
- PPS receives a CMISE negative response with the reason set to ‘No Such Object Class’. This could include when the PPS object instances on the far-end of the protection group or protection group unit are not created.
- The configuration between the AccessNode OPC and the SuperNode is not supported. The following configurations are two examples of this.
  - — The AccessNode is configured for the host representing the SuperNode, using GR-303 multi-vendor interface (MVI) protocol only, with no possibility of switching to the proprietary protocol GR-303 Digital Multiplex System (DMS). On the SuperNode, the integrated digital terminal (IDT), representing the AccessNode, is configured for proprietary protocol GR-303 DMS only.

    This configuration is reached by defining the host on the OPC as GR-303 MVI and by setting the RDTVAR field of RDTINV table to RFT on the SuperNode.
  - — The AccessNode is configured for the host representing the SuperNode, using either the GR-303 protocol MVI or the proprietary protocol GR-303 DMS. On the SuperNode, the IDT, representing the AccessNode is configured for GR-303 MVI only.

    This configuration is reached by defining the host on the OPC as GR-303 DMS and by setting the RDTVAR field of RDTINV table to GENTMC on the SuperNode.

Report severity

Warning.

Report format

The following is the format for the HMU311 log report.

```
HMU311 <date and time>
<Host Number> PPS: <Message text>
<Additional message text>
```

—continued—

HMU311, continued

Report example

The following is an example of the HMU311 log for a PPS message larger than 256 bytes.

```
HMU311 AUG12 08:44:36
Host: 0 PPS: GR-303 Message Size Invalid
Message larger than 256 bytes received
```

The following is an example of the HMU311 log for a path mismatch.

```
HMU311 AUG12 08:44:36
Host: 0 PPS: remote message received on EOC path
Request to switch TMC path. Mismatch detected

HMU311 AUG12 08:44:36
Host: 0 PPS: CMISE negative Response received
Path mismatch detected by far-end.
```

The following is an example of the HMU311 log for PPS objects not created on the far-end.

```
HMU311 AUG12 08:44:36
Host: 0 PPS: CMISE negative Response received
PPS Object <Object class number> not created on far-end.
```

The following is an example of the HMU311 log for configuration mismatch.

```
HMU311 AUG12 08:44:36
Host: 0 PPS: Invalid Message Received on Host Configured as
GR-303 Per GR-303 Standard, GR-303 Path Will be made Active or
is Active.
```

—continued—

HMU311, continued

Action

Step Action

PPS message larger than 256

1 If this message text occurs continually, verify that the message sent by the local digital switch (LDS) is correct. Refer to *Subscriber Carrier Module-100 Access Maintenance Manual*, 297-8251-550.

Path type mismatch

2 Verify that the DS1s are not reversed. Refer to the appropriate Installation Guide and *Subscriber Carrier Module-100 Access Maintenance Manual*, 297-8251-550.

3 Verify that the PPS objects are properly created on the far-end. Refer to *Subscriber Carrier Module-100 Access Maintenance Manual*, 297-8251-550.

PPS objects not created at the far-end

4 Verify the PPS objects are created on the far-end. Refer to *Subscriber Carrier Module-100 Access Maintenance Manual*, 297-8251-550.

Configuration mismatch

5 Determine the configuration to use: GR-303 MVI or GR-303 DMS (7-layer OSI).

- If GR-303 MVI is used, make sure that the host is defined as ‘GR-303 MVI’ on the OPC and IDT is defined as ‘GENTMC’ in table RDTINV (field RDTVAR) on the SuperNode. Refer to *Subscriber Carrier Module-100 Access Maintenance Manual*, 297-8251-550.
- If proprietary protocol is to be used, make sure that the host is defined as ‘GR-303 DMS’ on the OPC and the IDT is defined as ‘RFT’ in table RDTINV (field RDTVAR) on the SuperNode. Refer to *Subscriber Carrier Module-100 Access Maintenance Manual*, 297-8251-550.

—end—

HMU350

Report explanation

This log reports an error condition detected by the host messaging unit (HMU), which is one of two processors on the processor circuit pack.

> ***Note:*** The HMU cannot generate a log in a standard format, so the HMU sends the information to the access processing unit (APU) where it is formatted for standard log output. Therefore, all HMU logs have two headers: the first header always shows HMU350; the second header shows the actual number of the log report.

Report format

The following is the format for the HMU350 log report.

```
HMU350 mmm:dd hh:mm:ss nnnn INFO
HMU350 mmm:dd hh:mm:ss
Resource: <class> <instance>          Event: <event string> <text>
```

Report example

The following shows a typical example of the HMU350 log report.

```
HMU350 MAY:01 11:51:01 4100 INFO
HMU350 MAY01 11:51:38
Resource: LAPD 0         Event: Data Comm Loss of Signal
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<class> <instance>	CNET 0 SRMT 0 LAPD 0 OBIC 0 COMN 0 ***Note:*** All values represent major HMU resources, and all except LAPD represent actual hardware devices.	Two-part identifiers for HMU maintenance, which indicates the resource and instance. For example, in CNET 0, CNET is the resource, and 0 is the instance of the resource.
—continued—		

—continued—

HMU350, continued

Field	Value	Description
<event string>	There is a set of expected values for each of the above resource values: CNET: TBL_LAN_ENTER_FAIL TBL_SEV_INTERRUPT TBL_TBC_INTERRUPT TBL_JABBER_TIMEOUT TBL_TBC_CMD_TIMEOUT TBL_BUS_ERROR TBL_DUP_ADDRESS TBL_FAILED_HIT TBL_FAILED_FDLB TBL_FAULTY_TX SRMT: S01/R75 DEV ACC FAIL S01 TX FIFO UNDERRUN S01/R75 INIT CONFIG FAIL S01 RX SYNC LOSS S01 RX FIFO OVERRUN R75 MAJOR PAR ERR (SQA) R75 MAJOR BUS ERR (SQA) R75 MAJOR PAR ERR (PQA) R75 MAJOR BUS ERR (PQA) LAPD: loss of signal OBIC: OBIC DEV ACCESS FAIL OBIC INIT CONFIG FAIL COMN: Init Store error Init Error Init Bind Error Critical s/w Error	Event text. Describes the recently occurred HMU event. Usually a hardware failure; however in the case of LAPD, it describes an event associated with the protocol, such as a loss of signal.
<text>	Current values: – TBL initialization Failed (part of CNET LOG) – no peer connection (part of LAPD LOG)	This field is optional and will be of use only to the BNR design community to help them solve the problem quicker. It consists of more explanation text to give further detail on the failure that occurred. It will not exceed one line in length.
—end—		

—continued—

HMU350, continued

Action

The action to be taken depends on the text that appears in the Event field of the log report.

For the following events, replace the processor circuit pack (APC) as described in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

- TBL_SEV_INTERRUPT
- TBL_JABBER_TIMEOUT
- TBL_FAILED_HIT
- TBL_FAILED_FDLB
- TBL_FAULTY_TX
- TBL_MODEM_FAIL
- S01/R75 DEV ACC FAIL
- S01 TX FIFO UNDERRUN
- S01/R75 INIT CONFIG FAIL
- S01 RX SYNC LOSS
- S01 RX FIFO OVERRUN
- R75 MAJOR PAR ERR (SQA)
- R75 MAJOR BUS ERR (SQA)
- R75 MAJOR PAR ERR (PQA)
- R75 MAJOR BUS ERR (PQA)
- OBIC DEV ACCESS FAIL
- OBIC INIT CONFIG FAIL

For the following events, investigate the connection across the network:

- loss of signal
- TBL_LAN_ENTER_FAIL

For the event TBL_DUP_ADDRESS, the APC has the same network address as some other node in the network. Contact field support for assistance.

For the event TBL_TBC_CMD_TIMEOUT, reset the APC. If another HMU350 log is generated with the same event text, replace the processor circuit pack as described in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5 C.

—continued—

HMU350, continued

Some HMU event reports describe failure scenarios due to NE communication attempts with the far end. For example, if a loss of signal is detected by the LAPD protocol, this event is reported through the LOGs; however there may be nothing wrong with the NE that reports the fault. As a default, forward all HMU event reports to Nortel Networks, along with a complete set of LOGs for further investigation.

—end—

HMU720

Report explanation

This log is generated when the HMU incurs a restart. A powerup or a manual reset of the APC card will generate a RELOAD SW RESTART log within one minute, and a COLD RESTART log from 5 to 10 minutes later. These two logs are normal and should be expected.

> ***Note:*** The HMU can not generate a log in a standard format, so the HMU sends the information to the access processing unit (APU) where it is formatted for standard log output. Therefore, all HMU logs have two headers: the first header always shows HMU720; the second header shows the actual number of the log report.

Report format

The following is the format for the HMU720 log report.

HMU720 mmm:dd hh:mm:ss nnnn INFO
HMU720 mmm:dd hh:mm:ss
<text>

Report example

The following shows a typical example of the HMU720 log report.

```
HMU720 MAY29 11:51:38 4100 INFO
HMU720 MAY29 01:23:45
RELOAD SW RESTART
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<text>	RELOAD SW RESTART COLD RESTART	Restart type

Action

If other restart logs appear after this log, and no powerup or manual reset have occurred, these logs should be forwarded to Nortel Networks for problem diagnosis and corrective action.

—end—

HMU900

Report explanation

This log is generated when an HMU sanity timeout occurs, when pSOS detects a fatal error, or when an HMU task traps.

> ***Note:*** The HMU can not generate a log in a standard format, so the HMU sends the information to the access processing unit (APU) where it is formatted for standard log output. Therefore, all HMU logs have two headers: the first header always shows HMU900; the second header shows the actual number of the log report.

Report format

The following is the format for the HMU900 log report.

```
HMU900 mmm:dd hh:mm:ss nnnn INFO
   severity HMU900 mmm:dd hh:mm:ss
   <errno> <type> <vector> <taskname>
   <statusreg>
   <illaddr>
   <traceback>
```

Report example

The following are typical examples of the HMU900 log report.

```
HMU900 MAY01 11:51:38 4100 INFO
   *** HMU900 MAY29 01:23:45
   UNEXPECTED EXCEPTION

HMU900 MAY01 11:51:38 4200 INFO
   *** HMU900 MAY29 01:23:45
   SANITY TIMEOUT vector = 1f

HMU900 MAY01 11:51:38 4300 INFO
   *** HMU900 MAY29 01:23:45
   errno = 1961 FATAL ERROR
   006108b4
   0063d1e4
   deaddead
```

—continued—

HMU900, continued

```
HMU900 MAY01 11:51:38 4400 INFO
   *** HMU900 MAY29 01:23:45
   BUS ERROR vector = 2 task name = 00170000
   sr = 3000
   ill addr =0
   006108b4
   0063d1e4
   deaddead
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<errno>	int32 in decimal	The error number. This field exists only if <type> is FATAL ERROR or EXIT. If type is FATAL ERROR, <errno> is the return code from pSOS. If <type> is EXIT, <errno> is the return code from the task.
<type>		The error type can take the following values:
	UNEXPECTED EXCEPTION	– unexpected exception
	SANITY TIMEOUT	– sanity timeout
	FATAL ERROR	– pSOS fatal error
	EXIT	– task exit
	PARITY ERROR	– parity error while the HMU is master of the bus
	BUS ERROR	– bus error task trap
	ADDRESS ERROR	– address error task trap
	ILLEGAL INSTRUCTION	– illegal instruction task trap
	DIVIDE BY ZERO	– divide by zero task trap
	PRIVILEGE VIOLATION	– privilege violation task trap
<vector>	int32 in decimal	The vector number corresponding to the task trap. Present only if< type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.

—continued—

—continued—

HMU900, continued

Field	Value	Description
<taskname>	int32 in hex, or 4 alphanumeric characters	The name or id of the task that trapped. Present only if <type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.
<statusreg>	int16 in hex	The contents of the CPU status register when the trap has occurred. Present only if<type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.
<illaddr>	int32 in hex	The illegal address that caused the bus or address task trap. Present only if <type> is BUS ERROR or ADDRESS ERROR.
<traceback>	set of int32 in hex, normally terminated by "deaddead".	Set of addresses showing the nesting of functions when the software error occurred. Present only if <type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.
—end—		

Action

This log should be forwarded to Nortel Networks for problem diagnosis and corrective action.

—end—

HMU901

Report explanation

This log is generated by HMU applications whenever a software error is detected. A software error is an unexpected software condition, such as out of bound input arguments passed to a function.

> ***Note:*** The HMU can not generate a log in a standard format, so the HMU sends the information to the access processing unit (APU) where it is formatted for standard log output. Therefore, all HMU logs have two headers: the first header always shows HMU901; the second header shows the actual number of the log report.

Report format

The following is the format for the HMU901 log report.

```
HMU901 mmm:dd hh:mm:ss nnnn INFO
   HMU901 mmm:dd hh:mm:ss
   <sectionName> <lineNumber>
   <traceback>
   (|string|) <int32>
```

Report example

The following shows a typical example of the HMU901 log report.

```
HMU901 MAY 01 11:51:38 4100 INFO
   ** HMU901 MAY12 12:34:56
   hmfmi2.ab01 1961
   0061dece
   0061b230
   006638b8
   0061ad5e
   0061b0bc
   deaddead
   1

HMU901 MAY 01 11:51:38 4100 INFO
   ** HMU901 MAY12 12:34:56
   hmfmi2.ab01 1961
   0061dece
   0061b230
   006638b8
   0061ad5e
   0061b0bc
   deaddead
   Cannot allocate memory 2
```

—continued—

HMU901, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<sectionName>	alphanumeric	Section name
<lineNumber>	numeric	Line number
<traceback>	set of int32 in hex, normally terminated by “deaddead”	Set of addresses showing the nesting of functions when the software error occurred.
<string>	string of characters	Optional field. String of characters provided by the application which generates the SWERR, to give some indication about the software error.
<int32>	int32 in decimal	Application-generated long word data, to give some information about the software error (typically a bad return code).

Action

This log should be forwarded to Nortel Networks for problem diagnosis and corrective action.

—end—

IRTU300

Report explanation

This log indicates that a fault has been generated by the Integrated Remote Test Unit (IRTU). Information about test head 2 is available for model NT4K57AB only.

Report format

The following is the format for the IRTU300 log report.

IRTU300 mmm:dd hh:mm:ss nnnn event_type event_label
   Resource: <class> Event: <event>

Report example

The following shows typical examples of the IRTU300 log report.

```
IRTU300 MAY01 11:51:38 4100 TBL IRTU Fault
Resource: Test Head 1      Event: Total Failure

IRTU300 MAY01 11:56:21 4300 TBL IRTU Fault
Resource: Test Head 2      Event: 2W Calibration

IRTU300 MAY01 11:53:45 4200 TBL IRTU Fault
Resource: Digital          Event: TAC MOH Clock lost
```

—continued—

IRTU300, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<class>	System Digital Test Head 1 Test Head 2 Test Head Mgr PUPS	
<event >	Software Fault Parity Error Task Memory Full General Memory Full TAC MOH Clock Lost IDP Out of Time IDP Sanity Timeout Partial Failure Total Failure 2W Calibration 4W Calibration WB Calibration 2W Diagnostics 4W Diagnostics WB Diagnostics Fatal Swerr PUPS Failure	

Action

If the event field indicates TAC MOH Clock Lost, do whatever is necessary to put the TAC back into service.

—end—

IRTU301

Report explanation

This log indicates that a warm, cold or reload restart of the IRTU has failed for some reason. The log is generated when the IRTU goes to a Load Fail or Total Fail state.

Report format

The following is the format for the IRTU301 log report.

IRTU301 mmm:dd hh:mm:ss nnnn event_type event_label
Reason: <reason>   Problem id: <id number>

Report example

The following shows a typical example of the IRTU301 log report.

```
IRTU301 MAY01 11:51:38 4100 TBL IRTU Restart Fail
Reason: Load Failed          Problem id: 407
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<reason>	Load Failed Hardware Init Failed OPC Comm Failed Load Corrupted Aborted Init Message Timeout Software not loaded	
<id number>	Decimal number	Identification number of problem

Action

If the reason field indicates Load Failed**,** try a different IRTU software load. If the log is generated again, try replacing the IRTU.

If the reason field indicates Hardware Init Failed, replace the IRTU.

If the reason field indicates OPC Comm Failed, the link between the OPC and processor is down. Try downloading the IRTU again. If the problem still persists, check the links.

—continued—

IRTU301, continued

If the reason field indicates Load Corrupted, try a different IRTU software load. If the log is generated again, replace the IRTU.

If the reason field indicates Aborted, an event interrupted the downloading process. Try a different IRTU software load, and if the problem persists, replace the IRTU.

If the reason field indicates Init Message Timeout, an event caused the load to fail after it was downloaded to the IRTU. Try a different IRTU software load, and if the problem persists, replace the circuit pack.

If the reason field indicates Software not loaded, the RMM tried to perform a reload on the IRTU but found that there was no software loaded. In this case the IRTU is automatically downloaded. No action is required.

—end—

IRTU500

Report explanation

This log indicates that the IRTU card has been physically removed from the shelf.

Report format

The following is the format for the IRTU500 log report.

IRTU500 mmm:dd hh:mm:ss nnnn event_type event_label
NE: <ne id> <ne name>
Shelf: <shelf type>
Slot: <slot number>
Card type: IRTU

Report example

The following shows a typical example of the IRTU500 log report.

```
IRTU500 SEP08 23:57:37 2200 INFO Card Removal
   NE:           1
   Shelf:        CE
   Slot:         21
   Card type:    IRTU
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<ne id>	Decimal number	Network element number
<ne name>	String	Network element name
<shelf type>	String	Shelf type
<slot number>	Decimal number	Slot where the card was removed

Action

None

—end—

IRTU501

Report explanation

This log indicates that the IRTU card has been reinserted into the shelf. This log will be generated only after the IRTU has been provisioned. It will not be generated the first time the card is inserted into the shelf.

Report format

The following is the format for the IRTU501 log report.

IRTU501 mmm:dd hh:mm:ss nnnn event_type event_label
NE: <ne id> <ne name>
Shelf: <shelf type>
Slot: <slot number>
Card expected: IRTU
Card inserted: <card inserted>
PEC: <PEC code>
Slot state: <slot state>

Report example

The following shows a typical example of the IRTU501 log report.

```
IRTU501 SEP08 23:57:37 0800 INFO Card Insertion
   NE:                 1
   Shelf:              CE
   Slot:               21
   Card expected:      IRTU
   Card inserted:      IRTU
   PEC:                NT4K57AA
   Slot state:         Equipped
```

—continued—

IRTU501, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<ne id>	Decimal number	Network element number
<ne name>	String	Network element name
<shelf type>	String	Shelf type
<slot number>	Decimal number	Slot where the card was removed
<card expected>	IRTU	IRTU card is expected
<card inserted>	IRTU Unknown	The IRTU card should be inserted. If a card other than the IRTU is inserted, “Unknown” will appear in the field.
<PEC code>	Alphanumeric code	Product equipment code for the inserted card
<slot state>	Equipped Mismatched	If the IRTU card is inserted, the field will display “Equipped”. If a card other than the IRTU was inserted into the slot, the field will display “Mismatched”.

Action

This log is generally for information only. However, if the card inserted field indicates Unknown, the wrong circuit pack was installed into the IRTU slot. In this case, remove the current circuit pack.

If the slot state indicates Mismatched, the wrong circuit pack was installed into the IRTU slot. In this case, remove the current circuit pack.

—end—

IRTU600

Report explanation

This log indicates that a warm, cold or reload restart of the IRTU has been successfully completed. The log will be generated after the IRTU720 log.

Report format

The following is the format for the IRTU600 log report.

IRTU600 mmm:dd hh:mm:ss nnnn event_type event_label
Restart Complete

Report example

The following shows a typical example of the IRTU600 log report.

```
IRTU600 SEP08 23:57:37 2200 INFO IRTU Restart Pass
   Restart Complete
```

Action

None

—end—

IRTU700

Report explanation

This log indicates that a fault generated by the IRTU has been cleared. Information about test head 2 is available for model NT4K57AB only.

Report format

The following is the format for the IRTU700 log report.

```
IRTU700 mmm:dd hh:mm:ss nnnn event_type event_label
   Resource: <class>      Event: <event>
```

Report example

The following shows a typical example of the IRTU700 log report.

```
IRTU700 AUG30 13:58:23 5400 INFO IRTU Fault Cleared
   Resource: Test Head 1     Event: 2W Diagnostics
```

—continued—

IRTU700, continued

Field descriptions

The following table explains each of the variable fields in this log report.

Field	Value	Description
<class>	System Digital Test Head 1 Test Head 2 Test Head Mgr PUPS	
<event>	Software Fault Parity Error Task Memory Full General Memory Full TAC MOH Clock Lost IDP Out of Time IDP Sanity Timeout Partial Failure Total Failure 2W Calibration 4W Calibration WB Calibration 2W Diagnostics 4W Diagnostics WB Diagnostics Fatal Swerr PUPS Failure	

Action

None

—end—

IRTU720

Report explanation

This log indicates that a reload restart is taking place on the IRTU. It is followed by an IRTU600 log.

Report format

The following is the format for the IRTU720 log report.

IRTU720 mmm:dd hh:mm:ss nnnn event_type event_label
<text>

Report example

The following shows a typical example of the IRTU720 log report.

```
IRTU720 AUG30 13:58:35 5500 INFO IRTU Restart
   Reboot In Progress
```

Action

None

—end—

LC300

Report explanation

A line card failure was detected. The system could not recover the line card.

Report format

The following is the format for the LC300 log report:

LC300 mmm:dd hh:mm:ss nnnn event_type event_label
Log text: Line Card Failure
Location fields. See Appendix A.

Report example

The following is a typical example of the LC300 log report:

```
LC300 MAY12 12:34:56 1234 INFO LC Fault
   Log text:         Line Card Failure
   NE:               12
   Location:         1
   Shelf:            CDS 1
   Slot:             11
   Service Class:    2-wireFXO
   Circuit Pack HW:  O2WO LC
```

Field descriptions

See Appendix A for location field variables.

Action

If this log is generated for an Epsilon line card and follows an LC602 log, check for the removal of the talk battery. Refer to the chapter “Interpreting an LED or lamp” in *Alarm and Trouble Clearing Procedures*, 323-3001-543, in *Maintenance*, Volume 5A, for a fail (red) LED on an Epsilon 2-wire station line card.

Otherwise, perform a line card reset from the network element user interface. If the line card fails the reset operation, replace the line card, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. If the reset passes and the line card is already provisioned, the line card returns to service automatically.

—end—

LC301

Report explanation

There is no longer synchronization between the line card and the NT1.

Report format

The following is the format for the LC301 log report:

```
LC301 mmm:dd hh:mm:ss nnnn event_type event_label
   Location fields. See Appendix A.
   Primary Power Status:        <pstatus>
   Secondary Power Status:      <sstatus>
```

Report example

The following is a typical example of the LC301 log report:

```
LC301 MAY12 12:34:56 1234 INFO NT1 Sync Loss
   NE:                      11
   Location:                1
   Shelf:                   CDS 1
   Slot:                    12
   Primary Power Status:    Out
   Secondary Power Status: Normal
```

Field descriptions

The following table explains the Primary Power Status and Secondary Power Status fields in this log report.

Field	Value	Description
<pstatus>	Out Normal	Last received status of the NT1 primary power supply before the log was generated.
<sstatus>	Out Normal	Last received status of the backup power supply.

Action

Troubleshoot the NT1 as instructed in the NT1 documentation.

—end—

LC302

Report explanation

The line card detected a power loss at the NT1.

Report format

The following is the format for the LC302 log report:

LC302 mmm:dd hh:mm:ss nnnn event_type event_label
Location fields. See Appendix A.
Primary Power Status: <pstatus>
Secondary Power Status: <sstatus>

Report example

The following is a typical example of the LC302 log report:

```
LC302 MAY12 12:34:56 1234 INFO NT1 Power Loss
   NE:                      11
   Location:                1
   Shelf:                   CDS 1
   Slot:                    13
   Primary Power Status:    Out
   Secondary Power Status:  Out
```

Field descriptions

The following table explains the Primary Power Status and Secondary Power Status fields in this log report.

Field	Value	Description
<pstatus>	Out Normal	Last received status of the NT1 primary power supply before the log was generated
<sstatus>	Out Normal	Last received status of the backup power supply

Action

Troubleshoot the NT1 as instructed in the NT1 documentation.

—end—

LC303

Report explanation

The line card detected a change in status on one or both of the NT1 power supplies.

Report format

The following is the format for the LC303 log report:

LC303 mmm:dd hh:mm:ss nnnn event_type event_label
Location fields. See Appendix A.
Primary Power Status: <pstatus>
Secondary Power Status: <sstatus>

Report example

The following is a typical example of the LC303 log report:

```
LC303 MAY12 12:34:56 1234 INFO NT1PSChanged
   NE:                        11
   Location:                  1
   Shelf:                     CDS 1
   Slot:                      13
   Primary Power Status:      Normal
   Secondary Power Status:    Out
```

Field descriptions

The following table explains the Primary Power Status and Secondary Power Status fields in this log report.

Field	Value	Description
<pstatus>	Out Normal	Last received status of the NT1 primary power supply before the log was generated
<sstatus>	Out Normal	Last received status of the backup power supply

Action

Troubleshoot the NT1 as instructed in the NT1 documentation.

—end—

LC304

Report explanation

The line card detected a change in status of the NT1 test mode.

Report format

The following is the format for log report LC304:

LC304 mmm:dd hh:mm:ss nnnn event_type event_label
Location fields. See Appendix A.
NT1 Test Mode: <mode>

Report example

The following is a typical example of log report LC304:

```
LC304 MAY12 12:34:56 1234 INFO NT1TMChanged
   NE:                   11
   Location:             1
   Shelf:                CDS 1
   Slot:                 13
   NT1 Test Mode:        Under Test
```

Field descriptions

The following table explains the NT1 Test Mode field in this log report.

Field	Value	Description
<mode>	Under Test In Service	Current test mode of NT1

Action

If NT1 is under test, determine why it is in test mode.

If NT1 is in service, verify that the U-loop is activated.

—end—

LC307

Report explanation

The line card failed manual diagnostic testing. The body of the log report indicates the reason for the failure.

Report format

The following is the format for the LC307 log report:

LC307 mmm:dd hh:mm:ss nnnn event_type event_label
Log text: Line Card Diagnostic Failure
Reason: <reason>
Location fields. See Appendix A.

Report example

The following is a typical example of the LC307 log report:

```
LC307 MAY12 12:34:56 1234 INFO LC Diags
Log text: Line Card Diagnostic Failure
Reason: Analog Diagnostic Failure
   NE:                  11
   Location:            1
   Shelf:               CDS 3
   Slot:                11
   Circuit Pack HW:     O2WS LC
```

Field descriptions

The following table explains the Reason field in this log report.

Field	Value	Description
<reason>	One of the following text strings: Digital Diagnostic Failure Analog Diagnostic Failure TAC Communication Failure IDPROM Test Failure Internal Software Error Corrupted IDPROM Unable to Complete Test Bus Unavailable User Initiated Abort	Reason for the diagnostic failure

Action

Run diagnostics on the failed line card again. If the diagnostics fail again, replace the line card, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—end—

LC308

Report explanation

The line card did not return to service.

Report format

The following is the format for the LC308 log report:

LC308 mmm:dd hh:mm:ss nnnn event_type event_label
Log Text: Line Card Loading Failure
Reason: <reason>
Location fields. See Appendix A.

Report example

The following is a typical example of the LC308 log report:

```
LC308 MAY12 12:34:56 1234 INFO LC Load
   Log Text: Line Card Loading Failure
   Reason: Loading failed
   NE:                 11
   Location:           1
   Shelf:              CDS 3
   Slot:               11
   Circuit Pack HW:    O2WS LC
```

Field descriptions

The following table explains the Reason field in this log report.

Field	Value	Description
<reason>	One of the following text strings: Requested Load not Available Corrupted Load Communication Error	Reason for the diagnostic failure

Action

Ensure that the line card load context is correct, and that the line card load exists on the OPC. From the network element user interface run diagnostics on the line card. If diagnostics fail, replace the line card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—end—

LC401

Report explanation

This log reports the outcome of creating or deleting a line termination object (line card).

Report format

The following is the format for the LC401 log report:

LC401 mmm:dd hh:mm:ss nnnn event_type event_label
Log Text: Line Termination Action
Result: <result>
Location fields. See Appendix A.

Report example

The following shows a typical example of the LC401 log report:

```
LC401 MAY12 12:34:56 1234 INFO Create/Delete
   Log Text:                 Line Termination Action
   Result:                   Add Completed
   NE:                       11
   Location:                 1
   Shelf:                    CDS 2
   Slot:                     12
   Service Class:            2-WireFXO
   Circuit Pack HW:          O2WO
```

Field descriptions

The following table explains the Result field in this log report.

Field	Value	Description
<result>	One of the following text strings: Add Completed Add Fail Bad CRV Add Failed Add Rejected Delete Completed Delete Failed Delete Rejected	Result of the create/delete action

—continued—

LC401, continued

Action

If the result field indicated Add Completed or Delete Completed, no action is required.

If the result field indicated Add Fail Bad CRV, a provisioning request from a GR-303 host failed. Specifically, the

- GR-303 host attempted to provision a CRV (call reference value) that does not exist on the AccessNode.
- Shelf field indicates the GR-303 host that requested the failed provisioning add.
- Slot field indicates the CRV sent by the GR-303 host.

Edit the CRV using MVIPROV (sub-command editcrv) to commission the CRV on the AccessNode.

If the result field indicated Add Failed or Delete Failed, a database access failure was detected and provisioning should be redone. If this log persists, check for database error logs.

If the result field indicated Add Rejected or Delete Rejected, some type of inconsistency was detected. The inconsistency can be

- a line card provisioned with an invalid service class
- an attempt to edit attributes on an in-service line card
- an attempt to delete a line card not yet created (added).

See line card provisioning procedures in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

—end—

LC403

Report explanation

This log reports the outcome of the line card edit action.

If the line card is provisioned by a DMS-10NA switch, this log also reports the outcome of automatic line card edit actions caused by DMS Access call processing messages received from the DMS-10NA switch.

Report format

The following is the format for the LC403 log report:

LC403 mmm:dd hh:mm:ss nnnn event_type event_label
  Log Text: Line Termination Action
  Result: <result>
  Location fields. See Appendix A.

Report example

The following shows a typical example of the LC403 log report:

```
LC403 MAY12 12:34:56 1234 INFO Edit
   Log Text:             Line Termination Deprovisioning
   Result:               Edit Completed
   NE:                   11
   Location:             2
   Shelf:                CDS 2
   Slot:                 12
   Service Class:        2-WireFXO
   Circuit Pack HW:      O2WO LC
```

Field descriptions

The following table explains the Result field in this log report.

Field	Value	Description
<result>	One of the following text strings: Edit Completed Edit Failed Edit Rejected	Result of the line card edit action

—continued—

LC403, continued

Action

Edit Completed

If the line card was not provisioned by a DMS-10NA switch and the Result field indicates Edit Completed, no action is required.

Line cards provisioned by a DMS-10NA switch

If the line card is not an Epsilon or ExpressLine line card and the result field indicates Edit Completed, no action is required.

If the line card is an Epsilon or ExpressLine line card and the result field indicates Edit Completed, check for log LC602.

If log LC602	Then
is reported	See LC602 on page LC-15.
is not reported	No action is required.

Edit Failed

If the result field indicates Edit Failed, a database access failure was detected and provisioning should be redone. If this log persists, check for database error logs.

Edit Rejected

If the result field indicates Edit Rejected, some type of inconsistency was detected. The inconsistency can be

- a line card provisioned with an invalid service class
- an attempt to edit attributes on an in-service line card
- an attempt to delete a line card not yet created (added).

See line card provisioning procedures in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

—end—

LC500

Report explanation

A line card has been removed from a line drawer in a copper-distribution shelf.

Report format

The following is the format for the LC500 log report:

LC500 mmm:dd hh:mm:ss nnnn event_type event_label
  Log Text: Line Card Removed
  Location Information. See Appendix A.

Report example

The following shows a typical example of the LC500 log report:

```
LC500 MAY12 12:34:56 1234 INFO LC Removal
   Log Text:             Line Card Removed
   NE:                   11
   Location:             1
   Slot:                 12
   Service Class:        FXO
   Circuit Pack HW:      O2WO LC
```

Field descriptions

See Appendix A for a description of the location fields.

Action

Verify that the line card should have been removed. If it was not supposed to have been removed, reinstall the line card in the line drawer.

—end—

LC501

Report explanation

A scheduled audit has successfully restored a failed line card back to service.

Report format

The following is the format for the LC501 log report:

LC501 mmm:dd hh:mm:ss nnnn event_type event_label
Log Text: Bad Line Card Restored
Location Information. See Appendix A.

Report example

The following shows a typical example of the LC501 log report:

```
LC501 MAY12 12:34:56 1234 INFO LC Removal
   Log Text:            Bad Line Card Restored
   NE:                  11
   Location:            1
   Slot:                12
   Service Class:       FXO
   Circuit Pack HW:     O2WO LC
```

Field descriptions

See Appendix A for a description of the location fields.

Action

Verify that a failed line card has been restored to the in-service state.

—end—

LC502

Report explanation

User action has changed the primary state of the line termination from out of service (OOS) to in service (IS), or IS to OOS.

Report format

The following is the format for the LC502 log report:

```
LC502 mmm:dd hh:mm:ss nnnn event_type event_label
   Log Text: Service State Changed
   Present State:           <pres state>
   Previous State:          <prev state>
   Location fields. See Appendix A.
```

Report example

The following shows a typical example of the LC502 log report:

```
LC502 MAY12 12:34:56 1234 INFO State Change
   Log Text: Service State Changed
   Present State:            OOS
   Previous State:           IS
   NE:                       11
   Shelf:                    CDS 2
   Slot:                     4
   Service Class:            COINCT
   Circuit Pack HW:          O2WO LC
```

Field descriptions

See Appendix A for a description of the location fields.

Action

None

—end—

LC602

Report explanation

This log identifies a successful line card diagnostic and gives information about line card conditions.

Report format

The following is the format for the LC602 log report:

LC602 mmm:dd hh:mm:ss nnnn event_type event_label
Log Text: Information
Info:<info>
Location fields. See Appendix A.

Report example

The following shows a typical example of the LC602 log report:

```
LC602 MAY12 12:34:56 1234 INFO Line Card Info
   Log Text:             Information
   Info:                 Diagnostic Passed: Long
   NE:                   11
   Location:             1
   Shelf:                CDS 1
   Slot:                 42
   Service Class:        EBS
   Circuit Pack HW:      O2WS LC
```

Field descriptions

The following table explains the Info field in this log report.

Field	Value	Description
<info>	One of the following text strings: Diagnostics Passed: Long Diagnostics Passed: Short LC Hardware Mismatch - MVIPOTS on Epsilon AA Line Card Line Card Hardware Mismatched Loading Threshold Reached: LC hardware/software error Log Throttling Started: LC Protection Off Detected Log Throttling Started: LC Protection On Detected Maintenance Status Mismatch: Auto Recovery Initiated Mismatch Detected - MVIPOTS provisioned with Groundstart Service Failure: Fault Detected - Auto Recovery Initiated Service Failure: Loop Fault - Auto Recover Not Initiated	The information being reported by the log

—continued—

LC602, continued

Action

Diagnostics Passed: Short

If the Info field indicates Diagnostics Passed: Short, the test access card (TAC) was not detected. If long diagnostics are desired, verify that the TAC is installed and in service, and run long diagnostics again.

LC Hardware Mismatch - MVIPOTS on Epsilon AA Line Card

If the Info field indicates LC Hardware Mismatch - MVIPOTS on Epsilon AA Line Card, the NT4K65AA Epsilon line card has been provisioned for an MVIPOTS line, which is the POTS version for GR-303 MVI. This version of the Epsilon line card cannot support MVIPOTS. You must use an NT4K67AB or NT4K67AC Omega 2 wire line card for MVIPOTS to go into service.

Line Card Hardware Mismatched

If the Info field indicates Line Card Hardware Mismatched and the line card was not provisioned by a DMS-10NA switch, check the service provisioned on the slot. Replace the line card with the correct line card type.

Line cards provisioned by a DMS-10NA switch

If the Info field indicates Line Card Hardware Mismatched and the line card was provisioned by a DMS-10NA switch, check the line card type of the line card.

If the line card type is	Then
an Epsilon line card	See the “Epsilon and ExpressLine line cards” heading.
an ExpressLine line card	See the “Epsilon and ExpressLine line cards” heading.
any other line card type	Check the service provisioned on the slot and replace the line card with one of the correct line card type.

—continued—

LC602, continued

Line Card Hardware Mismatched (continued)

Epsilon and ExpressLine line cards

CAUTION
Loss of service
The reprovisioned Epsilon or ExpressLine line card is now in a mismatched state and cannot process any calls.

Epsilon and ExpressLine cards on a DMS-10NA switch can only be provisioned as LoopStart POTS.

This log report indicates that the line card was either:

- provisioned for POTS service and automatically reprovisioned for COIN service by DMS Access call processing
- provisioned for Loop Start service and manually reprovisioned for Ground Start service using the VLCM command interface.

Action

Do one of the following:

- Reprovision the Epsilon or ExpressLine line card as LoopStart POTS at the switch and the AccessNode
- Replace the line card with the correct line card type for the service provisioned on the slot

Loading Threshold Reached: LC hardware/software error

If the Info field indicates Loading Threshold Reached, the maximum number of attempts to load a line has been reached without success. The card is declared faulty and set as Test Failed. An hourly audit attempts to return the line to service. If required, you can determine faults manually by running diagnostics or try resetting the line card from the MAPCI.

Log Throttling Started: LC Protection Off Detected

If the Info field indicates Log Throttling Started: LC Protection Off Detected, the line card has gone out of protection mode. This report is for information only.

Log Throttling Started: LC Protection On Detected

If the Info field indicates Log Throttling Started: LC Protection On Detected, the line card has gone into protection mode. This report is for information only.

—continued—

LC602, continued

Maintenance Status Mismatch: Auto Recovery Initiated

If the Info field indicates Maintenance Status Mismatch, an in-service line was reloaded due to erroneous line card data. This report is for information only.

Service Failure: Fault Detected - Auto Recovery Initiated

If the info field indicates Service Fault: Fault Detected, the line card was either idle or carrying traffic when a major line card fault was detected. The fault causes diagnostics to be run on the card and a software reload. If a Line Card Failure log appears after this log, the line card could not be brought back in service. Look up the Line Card Failure log in this document and proceed accordingly.

Service Failure: Loop Fault - Auto Recover Not Initiated

If the Info field indicates Service Failure: Loop Fault, the line card passed diagnostics but the service load detected a loop error (such as fluctuating voltage). The card is marked Test Fail (TSTF). Inspect the tip and ring for odd connections.

—end—

NAD300

Report explanation

This log report indicates that the OPC rejected an X.25 connection request, because the request contained an invalid X.121 address.

Report severity

Warning

Report format

The following is the format for a NAD300 log report.

X.25 call rejected from OS, X.121 addr ‘<X.121 address>’.

Report example

The following is a typical example of a NAD300 log report.

```
NAD300 X.25 call rejected from OS, X.121 addr ‘A123456’.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<X.121 address>	Alphanumeric	Normally, the address of an operations support system attempting to access the OPC.

Action

Check with the OS system administrator and ensure that connection requests to the OPC contain a valid X.121 address, as defined in the OPC. X.121 addresses are defined in the OPC in a file having a pathname of /etc/x25init scc0. You can determine the X.121 address in this file by viewing it using the vi editor, or by following the procedure “Defining X.25 configuration parameters” in chapter 1 of *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A. Note that the execution of the above procedure will create a new x25init scc0 file.

If the X25 Interface Worksheet, located at the end of the above-noted chapter, has been used, you may find the X.121 address written down. However, this does not mean that the file contains the same value.

If the specified X.121 address is not being sent by any legitimate OS, this may indicate an unauthorized entry attempt. Take action appropriate for security violations.

—end—

NAD320

Report explanation

This log report indicates that problems were found in the execution of a scheduled audit of connection data. Inconsistencies in the data between an NE and the OPC are found, or the audit cannot be performed on an NE.

Report format

The following is the format for a NAD320 log report:

NAD320 Audited Connection.
Result: Failed.
The scheduled connection data audit <result>.

Report examples

The following is an example of a NAD320 log report:

```
NAD320 Audited Connections.
Result: Failed.
The scheduled connection data audit found inconsistent data at
NE(s) 1, 2 and 5.

NAD320 Audited Connections.
Result: Failed.
The scheduled connection data audit was unable to audit NE(s)
1, 2, and 5.

NAD320 Audited Connections.
Result: Failed.
The scheduled connection data audit found inconsistent data at
NE(s) 1, and 2 and was unable to audit NE(s) 5.

NAD320 Audited Connections.
Result: Failed.
The scheduled connection data audit was not executed due to a
system error.
```

—continued—

NAD320, continued

Field descriptions

Field	Value	Description
<result>	found inconsistent data at NE(s) <neid_list>	
	was unable to audit NE(s) <neid_list>	
	found inconsistent data at NE(s) <neid_list> and was unable to audit NE(s) <neid_list>	
	was not executed due to a system error	
<neid_list>	decimal number	NE identifier

Action

Step	Action
1	If data was found to be inconsistent at one or more network elements, use the "Audit connection data" command from the Utilities menu in the Connection Manager to correct the inconsistency by redistributing the connection data from the OPC to those network elements affected.
2	If the log indicated that the OPC was unable to audit one or more network elements, check and correct any communications problems between the OPC and network elements.Then use the "Audit connection data" command from the Utilities menu in the Connection Manager to correct the inconsistency by redistributing the connection data from the OPC to those network elements affected.
3	If the audit could not run, initiate a manual audit.

—end—

NAD321

Report explanation

This log report indicates the completion of an Add Connection operation from the STS Connection Manager. STS-1 connection data has been successfully updated at the OPC, but the connection could not be set up between the network elements.

The user-specified Connection ID and End Network Element (NE) names are included in the log report as reference to the STS-1 connection inventory maintained at the OPC. The list of NEs where the operation failed is included in the result indication.

The login name of the OPC user who performed the provisioning operation is also included in the log report for audit trail purposes.

Report severity

Minor

Report format

The following is the format for a NAD321 log report.

NAD321 Added STS-1 Connection.
Result: <result>
Connection Id: "<connection id>"
End NE A: "<ne id and name>"; End NE Z:"<ne id and name>"
Request initiated by user "<userid>".

Report example

The following is a typical example of a NAD321 log report.

```
NAD321 Added STS-1 Connection.
Result: Create but distribution failed unexpectedly.
Connection Id: "Main St King St 001"
End NE A: "2 MAIN"; End NE Z:"5 KING"
Request initiated by user "admin".
```

—continued—

NAD321, continued

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<result>		Indicates the results of the operation taken by the system on behalf of the user to complete the provisioning request.
	Created but distribution failed due to communication problems at NE(s) 2, 5	In this case, the STS-1 connection was added to the OPC connection inventory, but at least one NE could not be updated with this connection information.
	Retry distribution failed due to communication problems at NE(s) 2	In this case, an attempt to retry updating affected NEs immediately following a failed connection distribution has also failed at least one NE.
<connection id>	String	Indicates the STS-1 connection identifier.
<ne id and name>	String	Indicates the terminating network element number and name.
<userid>	String	Indicates name of the OPC user who requested this provisioning change.

Action

In addition to providing an STS-1 provisioning audit trial, these logs may require further investigation. Check the logs for a more recent, successfully completed connection audit log. If this log does not exist or it indicates inconsistencies at any network element, invoke a data connection audit from the STS Connection Manager utilities menu to determine if these inconsistencies still exist, and update the network element connection information if necessary.

—end—

NAD322

Report explanation

This log report indicates the completion of an Edit Connection operation from the STS Connection Manager. STS-1 connection data has been successfully updated at the OPC, but the connection could not be set up between the network elements.

The user-specified Connection ID and End Network Element (NE) names are included in the log report as reference to the STS-1 connection inventory maintained at the OPC. The list of NEs where the operation failed is included in the result indication.

The login name of the OPC user who performed the provisioning operation is also included in the log report for audit trail purposes.

Report severity

Minor

Report format

The following is the format for a NAD322 log report.

NAD322 Edited STS-1 Connection.
Result: <result>
Connection Id: "<connection id>"
End NE A: "<ne id and name>"; End NE Z:"<ne id and name>"
Request initiated by user "<userid>".

Report example

The following is a typical example of a NAD322 log report.

```
NAD322 Added STS-1 Connection.
Result: Edited but distribution failed due to communication
problems at NE(s) 2, 5.
Connection Id: "Main St King St 001"
End NE A: "2 MAIN"; End NE Z:"5 KING"
Request initiated by user "admin".
```

—continued—

NAD322, continued

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<result>		Indicates the results of the operation taken by the system on behalf of the user to complete the provisioning request.
	Edited but distribution failed due to communication problems at NE(s) 2, 5	In this case, the STS-1 connection was updated in the OPC connection inventory, but at least one NE could not be updated with this connection information.
	Retry distribution failed due to communication problems at NE(s) 2	In this case, an attempt to retry updating affected NEs immediately following a failed connection distribution has also failed at least on NE.
<connection id>	String	Indicates the STS-1 connection identifier.
<ne id and name>	String	Indicates the terminating network element number and name.
<userid>	String	Indicates name of the OPC user who requested this provisioning change.

Action

In addition to providing an STS-1 provisioning audit trial, these logs may require further investigation. Check the logs for a more recent, successfully completed connection audit log. If this log does not exist or it indicates inconsistencies at any network element, invoke a data connection audit from the STS Connection Manager utilities menu to determine if these inconsistencies still exist, and update the network element connection information if necessary.

—end—

NAD323

Report explanation

This log report indicates the completion of a Delete Connection operation from the STS Connection Manager. STS-1 connection data has been successfully updated at the OPC, but the connection could not be set up between the network elements.

The user-specified Connection ID and End Network Element (NE) names are included in the log report as reference to the STS-1 connection inventory maintained at the OPC. The list of NEs where the operation failed is included in the result indication.

The login name of the OPC user who performed the provisioning operation is also included in the log report for audit trail purposes.

Report severity

Minor

Report format

The following is the format of a NAD323 log report.

NAD323 Deleted STS-1 Connection.
Result: <result>
Connection Id: "<connection id>"
End NE A: "<ne id and name>"; End NE Z:"<ne id and name>"
Request initiated by user "<userid>".

Report example

The following is a typical example of a NAD323 log report.

```
NAD323 Added STS-1 Connection.
Result: Retry distribution failed due to communication problems
at NE(s) 5.
Connection Id: "Main St King St 001"
End NE A: "2 MAIN"; End NE Z:"5 KING"
Request initiated by user "admin".
```

—continued—

NAD323, continued

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<result>		Indicates the results of the operation taken by the system on behalf of the user to complete the provisioning request.
	Deleted but distribution failed due to communication problems at NE(s) 2, 5	In this case, the STS-1 connection was deleted to the OPC connection inventory, but at least one NE could not be updated with this connection information.
	Retry distribution failed due to communication problems at NE(s) 2	In this case, an attempt to retry updating affected NEs immediately following a failed connection distribution has also failed at least one NE.
<connection id>	String	Indicates the STS-1 connection identifier.
<ne id and name>	String	Indicates the terminating network element number and name.
<userid>	String	Indicates name of the OPC user who requested this provisioning change.

Action

In addition to providing an STS-1 provisioning audit trial, these logs may require further investigation. Check the logs for a more recent, successfully completed connection audit log. If this log does not exist or it indicates inconsistencies at any network element, invoke a data connection audit from the STS Connection Manager utilities menu to determine if these inconsistencies still exist, and update the network element connection information if necessary.

—end—

NAD324

Report explanation

This log report indicates the completion of a Scheduled connection data audit from the STS Connection Manager. The STS-1 connection audit of all NEs managed by the OPC has either found inconsistencies (OPC and NE connection data do not match) or it was unable to audit an NE, or both.

The user-specified Connection ID and End Network Element (NE) names are included in the log report as reference to the STS-1 connection inventory maintained at the OPC. The list of NEs where the operation failed is included in the result indication.The login name of the OPC user who performed the provisioning operation is also included in the log report for audit trail purposes.

Report severity

Critical if inconsistent data found. Major if unable to perform audit.

Report format

The following is the format of a NAD324 log report.

NAD324 Audit STS-1 Connection.
Result: Failed.
The scheduled connection data audit <result>.

Report example

The following are typical examples of a NAD324 log report.

```
NAD324 Audit STS-1 Connection.
Result: Failed.
The scheduled connection data audit found inconsistent data at
NE(s) 1, and 2.

NAD324 Audit STS-1 Connection.
Result: Failed.
The scheduled connection data audit was unable to audit NE(s)
1, and 2.

NAD324 Audit STS-1 Connection.
Result: Failed.
The scheduled connection data audit found inconsistent data at
NE(s) 1, and 2 and was unable to audit NE(s) 2.
```

—continued—

NAD324, continued

```
NAD324 Audit STS-1 Connection.
Result: Failed.
The scheduled connection data audit was not executed due to a
system error.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<result>	found inconsistent data at NE(s) <neid list> was unable to audit at NE(s) <neid list> found inconsistent data at NE(s) <neid list> and was unable to audit NE(s) <neid list> was not executed due to a system error	
<neid list>	decimal number	Network element identifier

Action

If the log indicates that connection data was found to be inconsistent at one or more NEs, use the “Audit connection data” command (from the Utilities menu in the STS Connection Manager) to re-distribute the OPC’s connection data to the affected NEs.

If the log indicates that the OPC was unable to audit one or more NEs, check any communication problems between the OPC and NEs and then use the same action as above.

If the audit could not run, initiate a manual audit.

—end—

NAD325

Report explanation

This log report indicates that one or more network elements (NEs) were not successfully updated with STS-1 connection data from the OPC. It also identifies any network elements where the data was received.

This activity was manually initiated by selecting the “Audit connection data” command from the Utilities menu in the STS Connection Manager. This is the normal corrective action when inconsistent data is reported by log report NAD325.

Report severity

Minor

Report format

The following is the format for a NAD325 log report.

NAD325 Correct STS-1 Connection.
Result: Failed.
The request to update connection data at NE(s) <ne list> failed due to communication problems. The request did succeed at NE(s) <ne list>.

Report example

The following is a typical example of a NAD325 log report.

```
NAD325 Correct STS-1 Connection.
Result: Failed.
The request to update connection data at NE(s) 1 and 2 failed
due to communication problems.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne list>	Set of decimal numbers	Set of network element identifiers

Action

Check to ensure that associations between the OPC and the listed NEs are up, correct communication problems as necessary, then reinstate the manual audit.

—end—

NAD326

Report explanation

This log report indicates that the attempt to enable STS-1 Connection Services for the given configuration could not be completed.

Report severity

Warning

Report format

The following is the format for a NAD326 log report.

NAD326 Enable STS-1 Connection Services action failed for configuration with endpoints at NE A: <NEA id> and NE Z: <NEZ id>. Please retry operation when associations to above NEs have been re-established.

Report example

The following is a typical example of a NAD326 log report.

```
NAD326 Enable STS-1 Connection Services action failed for
configuration with endpoints at NE A:1001 and NE Z:1002. Please
retry operation when associations to above NEs have been
re-established.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	**Value**	**Description**
<NEA id>	1-32767 (in OPC's span of control)	NE id of the FCOT in a point-to-point configuration for which STS-1 Connection Services has failed to be enabled.
<NEZ id>	1-32767 (in OPC's span of control)	NE id of the RFT in a point-to-point configuration for which STS-1 Connection Services has failed to be enabled.

Action

Check the association states of the given NEs. Retry the command as soon as possible after communication to the NEs has been reestablished. If the problem persists, contact Nortel Networks support.

—end—

NAD327

Report explanation

This log report indicates that there is a mismatch between the STS-1 Connection Services status at the OPC and one or both NEs.

Report severity

Warning

Report format

The following is the format for a NAD327 log report.

NAD327 Connection Services status mismatch between OPC and configuration with endpoints at NE A: <NEA id> and NE Z: <NEZ id>.

Report example

The following is a typical example of a NAD327 log report.

```
NAD327 Connection Services status mismatch between OPC and
configuration with endpoints at NE A:1001 and NE Z:1002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<NEA id>	1-32767 (in OPC’s span of control)	NE id of the FCOT in a point-to-point configuration for which STS-1 Connection Services was once enabled.
<NEZ id>	1-32767 (in OPC’s span of control)	NE id of the RFT in a point-to-point configuration for which STS-1 Connection Services was once enabled.

Action

A mismatch can occur under several circumstances. One circumstance is if an attempt to enable STS-1 Connection Services failed and the problem NE has reestablished its association with the OPC but the enable action has not yet been reattempted. In this case, reattempt the enable action using the Commission NE Connectivity dialog in the Commissioning Manager tool.

—continued—

NAD327, continued

Another circumstance occurs when an NE that previously had STS-1 Connection Services enabled has auto-provisioned and now has its default mapper enabled. In this case, if you wish to recover the old connection information, use the “Re-enable connection Services” action in the Commissioning Manager, then use the manual audit in the STS Connection Manager. Or, if you wish to clean the NEs in this configuration so that they can be used elsewhere with default mapping enabled, delete all provisioning information using the Provisioning Manager, delete all connection information using the Connection Manager, and delete the Configuration using the Commissioning Manager. Both NEs will have to auto-provision for this to work.

—end—

NAD330

Report explanation

This log report is generated when an unpaired line termination is found for an FCOT/RFT pair.

Report severity

Minor

Report format

The following is the format for a NAD330 log report.

NAD330 No match for Line Termination at <NE type> <NE id> shelf <shelf> slot <slot>.

Report example

The following is a typical example of a NAD330 log report.

```
NAD330 No match for Line Termination at FCOT 32767 shelf 7 slot
96.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<NE type>	FCOT RFT	Identifies central or remote site where line termination is not paired.
<NE id>	Decimal number 1-32767	Identifies NE instance.
<shelf>	Decimal number 1-7	Identifies shelf number.
<slot>	Decimal number 1-96	Identifies slot number.

Action

Resolve using the Provisioning Manager. If circuits were set up through an external operations system, resolve accordingly.

—end—

NAD331

Report explanation

This log report is generated when a line termination is found for an RFT with no corresponding information path at the OPC.

Report severity

Minor

Report format

The following is the format for a NAD331 log report.

NAD331 No Circuit for Line Termination at RFT <NE id> <NE id> shelf <shelf> slot <slot>.

Report example

The following is a typical example of a NAD331 log report.

```
NAD331 No Circuit for Line Termination at RFT 32767 shelf 7 slot
96.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<NE id>	Decimal number 1-32767	Identifies NE instance
<shelf>	Decimal number 1-7	Identifies shelf number
<slot>	Decimal number 1-96	Identifies slot number

Action

Resolve using the Provisioning Manager. If circuits were set up through an external operations system, resolve accordingly.

—end—

NAD332

Report explanation

This log report is generated when an information path is found with no corresponding line termination.

Report severity

Minor

Report format

The following is the format for a NAD332 log report.

NAD332 No match for Line Termination for Circuit at RFT <NE id> shelf <shelf> slot <slot>.

Report example

The following is a typical example of a NAD332 log report.

```
NAD332 No Line Termination for Circuit at RFT 32767 shelf 7 slot
96.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<NE id>	Decimal number 1-32767	Identifies NE instance
<shelf>	Decimal number 1-7	Identifies shelf number
<slot>	Decimal number 1-96	Identifies slot number

Action

Resolve using the Provisioning Manager. If circuits were set up through an external operations system, resolve accordingly.

—end—

NAD333

Report explanation

This log report is generated when there is a slot mismatch between an information path and a corresponding line termination.

Report severity

Minor

Report format

The following is the format for a NAD333 log report.

NAD333 Slot match: Circuit with shelf <shelf> slot <slot> - Line Termination at <NE type> <NE id> shelf <shelf> slot <slot>.

Report example

The following is a typical example of a NAD333 log report.

```
NAD333 Slot match: Circuit with shelf 7 slot 96 - Line
Termination at FCOT 32767 shelf 7 slot 95.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<NE type>	FCOT RFT	Identifies the central or remote site
<NE id>	Decimal number 1-32767	Identifies NE instance
<shelf>	Decimal number 1-7	Identifies shelf number
<slot>	Decimal number 1-96	Identifies slot number

Action

Resolve using the Provisioning Manager. If circuits were set up through an external operations system, resolve accordingly.

—end—

NAD334

Report explanation

This log report is generated when two corresponding line terminations are provisioned (through TL1) with incompatible service types.

Report severity

Minor

Report format

The following is the format for a NAD334 log report.

NAD334 Incompatible Service Types: shelf <shelf> slot <slot> at FCOT <NE id> uses <service type> - shelf <shelf> slot <slot> at RFT <NE id> uses <service type>.

Report example

The following is a typical example of a NAD334 log report.

```
NAD334 Incompatible Service Types: shelf 7 slot 96 at FCOT 32766
uses COINCT - shelf 7 slot 96 at RFT 32767 uses COINCT.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<NE id>	Decimal number 1-32767	Identifies NE instance
<shelf>	Decimal number 1-7	Identifies shelf number
<slot>	Decimal number 1-96	Identifies slot number
<service type>	Service Code	Identifies the service type. Compatible service types are listed in the following tables.

Action

Resolve accordingly through the TL1 interface.

—continued—

NAD334, continued

The following table lists the valid RFT services for specific FCOT services. For details on the service codes, see *Line Card Provisioning Procedures*, 323-3001-315 and *Line Card Testing Procedures*, 323-3001-316 in *Operations, Administration, and Provisioning*, Volume 4B.

Line card type	**FCOT service (code)**	**Valid RFT service (codes)**
2-wire	2POTSCT	2POTSRT, 2VIRTUAL
	2FXO	4FXS, 2FXS, 6TDM1O, 6TDM2O
	2FXS	4FXO, 2FXO, 6TDM1S, 6TDM2S
	2DPO	2DPT, 6TDM1, 6TDM2
	2DPT	2DPO, 6TDM1, 6TDM2
	2DDS	4DDS
	2TOS	4TO, 4ETO, 2TOS, 2ETOS
	2ETOS	4TO, 4ETO, 2TOS, 2ETOS
	2UVGCT	2UVGRT
	2COINCT	2COINRT
	DS1	4DX, 4TO, 4ETO, 4FXO, 4DDS, 2FXO, 2FXS, 2DPT, 2DPO, 2TOS, 2ETOS, 6E&M1, 6E&M2, 6E&M3, 6PRL1, 6PLR2, 6TDM1, 6TDM2, 6TDM1S, 6TDM2S, DS1, MRD, PLAR
	PLAR	PLAR
	MRD	MRD
4-wire	4DX	4DX, 6E&M1, 6E&M2, 6E&M3, 6PLR1, 6PLR2, 6PLR3, 6TDM1, 6TDM2
	4TO	4TO, 4ETO, 2TOS, 2ETOS
	4ETO	4TO, 4ETO, 2TOS, 2ETOS
	4FXO	4FXS, 2FXS, 6TDM1O
	4FXS	4FXO, 3FXO, 6TDM1S
	4DDS	4DDS
6-wire	6E&M1	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2
	6E&M2	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2
	6E&M3	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2
	6PLR1	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2
	6PLR2	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2
	6TDM1	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2

—continued—

—continued—

NAD334, continued

Line card type	FCOT service (code)	Valid RFT service codes
6-wire	6TDM2	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2
	6TDM1O	4FXO, 2FXO, 6TDM1S, 6TDM2S
	6TDM1S	4FXS, 2FXS, 6TDM1O, 6TDM2O
	6TDM2O	4FXO, 2FXO, 6TDM1S, 6TDM2S
	6TDM2S	4FXS, 2FXS, 6TDM1O, 6TDM2O

—end—

The following table lists the valid FCOT services for specific RFT services. For details on the service codes, see *Line Card Provisioning Procedures*, 323-3001-315 and *Line Card Testing Procedures*, 323-3001-316 in *Operations, Administration, and Provisioning*, Volume 4B.

Line card type	RFT service (code)	Valid FCOT service (codes)
2-wire	2POTSRT	2POTSCT
	2FXO	4FXS, 2FXS, 6TDM1O, 6TDM20, DS1
	2FXS	4FXO, 2FXO, 6TDM1S, 6TDM2S, DS1
	2DPO	2DPT, 6TDM1, 6TDM2, DS1
	2DPT	2DPO, 6TDM1, 6TDM2, DS1
	2DDS	4DDS, DS1
	2TOS	4TO, 4ETO, 2TOS, 2ETOS, DS1
	2ETOS	4TO, 4ETO, 2TOS, 2ETOS, DS1
	2UVGCT	2UVGRT
	2COINCT	2COINRT
	DS1	DS1
	PLAR	PLAR, DS1
	MRD	MRD
	VIRTUAL	2POTSCT
4-wire	4DX	4DX, 6E&M1, 6E&M2, 6E&M3, 6PLR1, 6PLR2, 6PLR3, 6TDM1, 6TDM2, DS1
	4TO	4TO, 4ETO, 2TOS, 2ETOS, DS1
	4ETO	4TO, 4ETO, 2TOS, 2ETOS, DS1
	4FXO	4FXS, 2FXS, 6TDM1O, DS1
	4FXS	4FXO, 3FXO, 6TDM1S, DS1
	4DDS	4DDS, DS1

—continued—

—continued—

NAD334, continued

Line card type	RFT service (code)	Valid FCOT service (codes)
6-wire	6E&M1	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2, DS1
	6E&M2	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2, DS1
	6E&M3	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2, DS1
	6PLR1	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2, DS1
	6PLR2	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2, DS1
	6TDM1	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2, DS1
	6TDM2	4DX, 6E&M1, 6E&M1, 6E&M3, 6PLR1, 6PLR2, 6PRL3, 6TDM1, 6TDM2, DS1
	6TDM1O	4FXO, 2FXO, 6TDM1S, 6TDM2S, DS1
	6TDM1S	4FXS, 2FXS, 6TDM1O, 6TDM2O, DS1
	6TDM2O	4FXO, 2FXO, 6TDM1S, 6TDM2S, DS1
	6TDM2S	4FXS, 2FXS, 6TDM1O, 6TDM2O, DS1
	—end—	

—end—

NAD335

Report explanation

This log report is generated when a line termination has an invalid far end line termination value.

Report severity

Minor

Report format

The following is the format for a NAD335 log report.

NAD335 Invalid Far End Line Termination at <NE type> < NE id> shelf <shelf> slot <slot> for <configuration type>.

Report example

The following is a typical example of a NAD335 log report.

```
NAD335 Invalid Far End Line Termination at RFT 32767 shelf 7
slot 96 for UDLC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<NE type>	FCOT RFT	Identifies central or remote site
<NE id>	Decimal number 1-32767	Identifies NE instance
<shelf>	Decimal number 1-7	Identifies shelf number
<slot>	Decimal number 1-96	Identifies slot number
<configuration type>	UDLC DS1 TR08	Identifies the configuration type

Action

Resolve using the Provisioning Manager.

—end—

NAD341

Report explanation

This log report indicates that a new user account was created, but communication problems prevented it from being created on one or more network elements (NEs).

Report severity

Minor

Report format

The following is the format for a NAD341 log report.

NAD341 User <user id> created.

Report example

The following is a typical example of a NAD341 log report.

```
NAD341 User “sshum” created.
Result: Create partially successful.
OPC Group = “admin”.
Access added on NE(s) 4898.
Failed to update NE(s) 4899.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user id>	character string	User identifier

Action

Attempt to re-establish the connection to the failed NEs. Then, using the Centralized User Administration tool, manually issue a user profile data audit found under the Utilities tool menu.

—end—

NAD342

Report explanation

This log report indicates that the specified user account was deleted, but communication problems prevented it from being deleted on one or more network elements (NEs).

Report severity

Minor

Report format

The following is the format for a NAD342 log report.

NAD342 User <user id> deleted.

Report example

The following is a typical example of a NAD342 log report.

```
NAD342 User “jjones” deleted.
Result: Delete partially successful.
OPC Group = “slat”.
Access added on NE(s) 4898.
Failed to update NE(s) 4899.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user id>	character string	User identifier

Action

Attempt to re-establish the connection to the failed NEs. Then, using the Centralized User Administration tool, manually issue a user profile data audit found under the Utilities tool menu.

—end—

NAD343

Report explanation

This log report indicates that the specified user account was disabled, but communication problems prevented it from being disabled on one or more network elements (NEs).

Report severity

Minor

Report format

The following is the format for a NAD343 log report.

NAD343 User <user id> disabled.

Report example

The following is a typical example of a NAD343 log report.

```
NAD343 User “jjones” disabled.
Result: Disable partially successful.
OPC Group = “admin”.
Access added on NE(s) 1234, 1235.
Failed to update NE(s) 1236.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user id>	character string	User identifier

Action

Attempt to re-establish the connection to the failed NEs. Then, using the Centralized User Administration tool, manually issue a user profile data audit found under the Utilities tool menu.

—end—

NAD344

Report explanation

This log report indicates that the specified password was created, but communication problems prevented it from being created on one or more network elements (NEs).

Report severity

Minor

Report format

The following is the format for a NAD344 log report.

NAD344 User <user id> password updated.

Report example

The following is a typical example of a NAD344 log report.

```
NAD344 User “jjones” password updated.
Result: Password update partially successful.
OPC Group = “admin”.
Access added on NE(s) 1234.
Failed to update NE(s) 1235, 1236, 1237.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user id>	character string	User identifier

Action

Attempt to re-establish the connection to the failed NEs. Then, using the Centralized User Administration tool, manually issue a user profile data audit found under the Utilities tool menu.

—end—

NAD345

Report explanation

This log report indicates that the user account’s NE access list was modified, but communication problems prevented it from being disabled on one or more network elements (NEs).

Report severity

Minor

Report format

The following is the format for a NAD345 log report.

NAD345 User <user id> NE access list modified.

Report example

The following is a typical example of a NAD345 log report.

```
NAD345 User “sshum” NE access list modified.
Result: Modification partially successful.
Old NE access list = [1234,2], [1235,2], [1236,1]
New NE access list = [1235,1], [1236,1]
Failed to update NE(s) 1234
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user id>	character string	User identifier

Action

Attempt to re-establish the connection to the failed NEs. Then, using the Centralized User Administration tool, manually issue a user profile data audit found under the Utilities tool menu.

—end—

NAD346

Report explanation

On completion of a user profile data audit (which can be automatic or user initiated), this log report lists all network elements (NEs) in the OPC span of control that failed that audit because of communication problems.

Report severity

Minor

Report format

The following is the format for a NAD346 log report.

NAD346 Audited user profile data.

Report example

The following is a typical example of a NAD346 log report.

```
NAD346 Audited user profile data.
Result: Failed.
Unable to audit NE(s) 4898, 4899.
```

Action

Attempt to re-establish the connection to the failed NEs. Then, using the Centralized User Administration tool, manually issue a user profile data audit found under the Utilities tool menu.

—end—

NAD351

Report explanation

This log report indicates that performance data was not collected due to loss of communication with the network element. The cause of this failure should have been reported already.

Report severity

Minor

Report format

The following is the format for a NAD351 log report.

NAD351 Cannot collect performance data from NE <ne identifier>; link down.

Report example

The following is a typical example of a NAD351 log report.

```
NAD351 Cannot collect performance data from NE 43; link down.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element

Action

Check for COM type logs and take the action described for those logs. If no COM type log has been generated, check the status of communications with the network element (for example, check the loss- of-association icon in one of the surveillance tools).

The OPC will attempt to obtain the performance data not collected, during the next collection period. However, storage capacities on the network elements and the OPCs are limited, and performance data will be lost if the communications problem is not corrected quickly.

—end—

NAD352

Report explanation

This log report indicates that performance data has been discarded because inaccuracy of the real time clock prevents an accurate collection interval to be obtained. This may have occurred because of a major drift or failure of a real-time clock on the OPC or the network element. It may have occurred because the time zone offset has been specified incorrectly at the OPC or network element. Or it may have occurred because the backup OPC became active and its clock was not synchronized with the other OPC.

Report severity

Minor

Report format

The following is the format for a NAD352 log report.

NAD352 Performance data from NE <ne identifier> discarded; clock out of sync.

Report example

The following is a typical example of a NAD352 log report.

```
NAD352 Performance data from NE 43 discarded; clock out of sync.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element

Action

Determine which clocks or time zone offsets are incorrect, and perform the time change procedure as required. Although clock synchronization between primary and backup OPCs is a manual procedure, synchronization is essential for accurate performance measurements.

Network elements synchronize their clocks with the active OPC once a day, to avoid failure of performance data collection due to clock drift. The OPC is tolerant of clock drift within 5 minutes.

The OPC will attempt to obtain the performance data not collected, during the next collection period. However, storage capacities on the network elements and the OPCs are limited, and performance data will be lost if the communications problem is not corrected quickly.

—end—

NAD373

Report explanation

This log report indicates that a protection group contains a network element which has been decommissioned.

Report severity

Warning

Report format

The following is the format for a NAD373 log report.

NAD373 Decommissioned NE <ne identifier> in 1:N protect group <group name>. Please remove it from the protection group.

Report example

The following is a typical example of a NAD373 log report.

```
NAD373 Decommissioned NE 43 in 1:N protect group East. Please
remove it from the protection group.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<group name>	Text	Name given to the protection group

Action

Open the 1:N Protection Manager tool. Select the group name (given in the log) from the Group List in the main window and open the “Prot Grp Details” dialog by selecting **Prot Grp Details** from the list menu. Delete the decommissioned network element within this dialog. Note that a protection group must have a protection channel and at least one working channel assigned. Select OK and exit the tool.

—end—

NAD375

Report explanation

This log report indicates that protection group data in the OPC and in the specified network element do not match. The OPC's protection data is considered correct, and the network element data will be changed by the system, to be consistent with the OPC's data.

Report severity

Warning

Report format

The following is the format for a NAD375 log report.

NAD375 Inconsistent data in NE <ne identifier> of 1:N protect group <group name>. Attempting to correct NE data to match OPC data.

Report example

The following is a typical example of a NAD375 log report.

```
NAD375 Inconsistent data in NE 43 of 1:N protect group East.
Attempting to correct NE data to match OPC data.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	**Value**	**Description**
<ne identifier>	Decimal number	Serial number of the network element
<group name>	Text	Name given to the protection group

Action

None

—end—

NAD376

Report explanation

This log report indicates that the specified network element is currently provisioned with a protection scheme other than 1:N, although it has been assigned to a 1:N protection group on the OPC.

Report severity

Critical

Report format

The following is the format for a NAD376 log report.

NAD376 NE <ne identifier> contains inconsistent 1:N protection data for group <group name>. To correct, run ‘Force NE OPC data consistency’ on this protection group.

Report example

The following is a typical example of a NAD376 log report.

```
NAD376  NE 43 contains inconsistent 1:N protection data for
group East. To correct, run ‘Force NE OPC data consistency’ on
this protection group.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<group name>	Text	Name given to the protection group

Action

Open the 1:N protection manager. If the network element is supposed to be provisioned as 1:N, then run ‘Force NE OPC data consistency’ on the protection group. If the NE is not supposed to be provisioned as 1:N, then select ’Provision Group Details’ on the protection group and delete this NE.

—end—

NAD377

Report explanation

This log report indicates that the specified network element has been provisioned as having 1:N protection, but it does not belong to any 1:N protection group.

Report severity

Critical

Report format

The following is the format for a NAD377 log report.

NAD377 NE <ne identifier> is in 1:N protection mode, but does not belong to any 1:N protection group on the OPC. Please see OPC Troubleshooting Guide.

Report example

The following is a typical example of a NAD377 log report.

```
NAD377  NE 43 is in 1:N protection mode, but does not belong to
any 1:N protection group on the OPC. Please see OPC
Troubleshooting Guide.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element

Action

The correct action depends on whether this NE is supposed to be part of a 1:N protection group. If it is, then simply add it to the correct protection group using the 1:N Protection Manager.

If it is not part of any 1:N protection group, then its protection scheme needs to be reprovisioned from 1:N. Log into the network element. Deactivate the facility. Delete the facility object. Then add the same facility object. Now the protection scheme should be 1:1.

—end—

NAD378

Report explanation

This log may occur after restoring OPC data, and will follow some COM502 logs. The database contained a record of the OPC trying to delete this NE from a 1:N protection group. While attempting to determine the current protection scheme of the NE, a communications error was encountered.

Report severity

Warning

Report format

The following is the format for a NAD378 log report.

NAD378 NE <ne identifier> protection scheme unknown, due to communications problems. Log into NE and verify that protection scheme is not 1:N.

Report example

The following is a typical example of a NAD378 log report.

```
NAD378  NE 43 protection scheme unknown, due to communications
problems. Log into NE and verify that protection scheme is not
1:N.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element

Action

Diagnose the COM502 log report first. Then log into the NE and determine its protection scheme. If the protection scheme is 1:N, then follow the action given for the NAD377 log report. Otherwise, simply ensure that the desired protection scheme is provisioned on this NE.

—end—

NAD380

Report explanation

This log report indicates that network telemetry has been assigned to a network element which has been decommissioned.

Report severity

Warning

Report format

The following is the format for a NAD380 log report.

NAD380 Network Telemetry cannot be sent to decommissioned NE <ne identifier>. Please assign network telemetry to another NE.

Report example

The following is a typical example of a NAD380 log report.

```
NAD380 Network Telemetry cannot be sent to decommissioned NE 43.
Please assign network telemetry to another NE.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element

Action

In order for telemetry to be properly collected, you must identify another network element and assign collection of telemetry to it.

—end—

NAD389

Report explanation

This log report indicates that a new user account could not be created on the specified network element because insufficient memory was available.

Report severity

Major

Report format

The following is the format for a NAD389 log report.

NAD389 Failed in creating new <user identifier> on NE <ne identifier> because the NE database is full.

Report example

The following is a typical example of a NAD389 log report.

```
NAD389 Failed in creating new Fred on NE 43 because the NE
database is full.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

Contact your Nortel Networks customer service representative.

—end—

NAD390

Report explanation

This log report indicates that during the assignment of a user password, the OPC was unable to propagate the password to the specified network element. Since access to a network element requires a password, the specified user is unable to log into this network element. You will see an instance of this log for each network element which did not receive the password.

Report severity

Major

Report format

The following is the format for a NAD390 log report.

NAD390 Failed to assign password for <user identifier> on NE <ne identifier>.

Report example

The following is a typical example of a NAD390 log report.

```
NAD390 Failed to assign password for Fred on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	**Value**	**Description**
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

If this report is generated for many network elements, the recommended corrective action is to disable the user’s password and perform the password assignment again.

If this report is generated for only a few network elements, you should remove the user’s accessibility to each specified network element and then provide it again. The OPC sends the existing password to the network element at this time.

—end—

NAD391

Report explanation

This log report indicates that when a user password was disabled, the network element specified in the log did not receive the change. The user may still access this network element. You will see an instance of this log for each network element which did not receive the password disable command.

Report severity

Major

Report format

The following is the format for a NAD391 log report.

NAD391 Failed to disable password for <user identifier> on NE <ne identifier>.

Report example

The following is a typical example of a NAD391 log report.

```
NAD391 Failed to disable password for Fred on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	**Value**	**Description**
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

Remove the user’s accessibility to the specified network element. When access permission is restored, the indication that the password is disabled is sent to the network element. This will deny access to the network element until the password is enabled.

Alternatively, you can enable and then disable the password again.

—end—

NAD392

Report explanation

This log report indicates that the OPC was unable to remove the specified user account from the specified network element. The existence of the user account on the OPC and access to the specified network element, are not changed. You will see an instance of this log for each network element for which the delete operation failed. The user account is removed from all other network elements.

Report severity

Minor

Report format

The following is the format for a NAD392 log report.

NAD392 Failed to delete user <user identifier> from NE <ne identifier>.

Report example

The following is a typical example of a NAD392 log report.

```
NAD392 Failed to delete user Fred from NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

Try the Delete User operation again. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

—end—

NAD393

Report explanation

This log report indicates that the OPC has been unable to change the access class of the specified user to the specified network element. Access to other network elements is unaffected.

Report severity

Minor

Report format

The following is the format for a NAD393 log report.

NAD393 Failed to update <user identifier>'s command class on NE <ne identifier>.

Report example

The following is a typical example of a NAD393 log report.

```
NAD393 Failed to update Fred's command class on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

Try the operation again. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

—end—

NAD394

Report explanation

This log report indicates that the OPC was unable to provide accessibility to the specified network element by the specified user. The existence of the user account on the OPC and access to other network elements, are unaffected.

Report severity

Minor

Report format

The following is the format for a NAD394 log report.

NAD394 Failed to create user <user identifier> on NE <ne identifier>.

Report example

The following is a typical example of a NAD394 log report.

```
NAD394 Failed to create user Fred on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

Try the operation again. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

—end—

NAD395

Report explanation

This log report indicates that during a user password change, the OPC was unable to propagate the new password to the specified network element. This means that the old password remains active in this network element. You will see an instance of this log for each network element which did not receive the password.

Report severity

Minor

Report format

The following is the format for a NAD395 log report.

NAD395 Failed to update <user identifier>'s password on NE <ne identifier>.

Report example

The following shows a typical example of a NAD395 log report.

```
NAD395 Failed to update Fred's password on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

It is not possible to change the password on a single network element. You must change the password again (using the Password Update tool), or request the user to change it (using the Password Update tool). A different new password must be used. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

—end—

NAD396

Report explanation

This log report indicates that during a user password change, the OPC was unable to record the new value. The old password remains active on the OPC; but it is updated on all network elements which are accessible using this user account.

Report severity

Major

Report format

The following is the format for a NAD396 log report.

NAD396 Failed to update <user identifier>'s password on OPC. Retry later to keep the password consistent on OPC and NEs.

Report example

The following is a typical example of a NAD396 log report.

```
NAD396 Failed to update Fred's password on OPC. Retry later to
keep the password consistent on OPC and NEs.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user identifier>	Text	A user account name

Action

It is not possible to change the password on a single network element. You must change the password again (using the Password Update tool), or request the user to change it (using the Password Update tool). A different new password must be used. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

—end—

NAD397

Report explanation

This log report indicates that the specified user account could not be deleted, because a user was logged into the specified network element using the account. The account has been removed from other network element databases.

Report severity

Minor

Report format

The following is the format for a NAD397 log report.

NAD397 Failed to delete <user identifier> from NE <ne identifier>. This user is currently logged into this NE.

Report example

The following is a typical example of a NAD397 log report.

```
NAD397 Failed to delete Fred from NE 43. This user is currently
logged into this NE.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

You will not be able to complete this operation until the user has logged out of the specified network element. When this occurs, re-execute the Delete User procedure. When the account has been removed from all network elements, it will be removed from the OPC. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

If it is necessary to force the user off the system, execute the user forceoff procedure. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

—end—

NAD398

Report explanation

This log report indicates that the password of the specified user account could not be disabled on the specified network element, because a user was logged into that network element, using the account. The password is disabled on other network elements.

Report severity

Minor

Report format

The following is the format for a NAD398 log report.

NAD398 Failed to disable password for <user identifier> on NE <ne identifier>. This user is currently logged into this NE.

Report example

The following is a typical example of a NAD398 log report.

```
NAD398 Failed to disable password for Fred on NE 43. This user
is currently logged into this NE.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

You will not be able to complete this operation until the user has logged out of the specified network element. When this occurs, re-execute the Password Disable procedure. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

If it is necessary to force the user off the system, execute the user forceoff procedure. See *System Administration Procedures*, 323-3001-302 in *Operations, Administration, and Provisioning*, Volume 4A, for detailed procedures.

—end—

NAD399

Report explanation

This log report indicates that a password could not be assigned for the specified user account, because of a shortage of memory on the network element.

Report severity

Major

Report format

The following is the format for a NAD399 log report.

NAD399 Failed in assigning password for <user identifier> on NE <ne identifier> because the NE database is full. This user cannot access this NE.

Report example

The following is a typical example of a NAD399 log report.

```
NAD399 Failed in assigning password for Fred on NE 43 because
the NE database is full. This user cannot access this NE.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

Contact your Nortel Networks customer service representative.

—end—

NAD500

Report explanation

This log report indicates that the OPC has accepted an X.25 connection request from an operations support system.

Report severity

Warning

Report format

The following is the format for a NAD500 log report.

NAD500 X.25 call accepted from OS, X.121 addr ‘<X.121 address>’.

Report example

The following is a typical example of a NAD500 log report.

```
NAD500 X.25 call accepted from OS, X.121 addr ‘A123456’.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<X.121 address>	Alphanumeric	Address of an operations support system

Action

None

—end—

NAD501

Report explanation

This log report indicates that an operations support system connection to the OPC has been terminated.

Report severity

Warning

Report format

The following is the format for a NAD501 log report.

NAD501 X.25 call terminated from OS, X.121 addr ‘<X.121 address>’.

Report example

The following is a typical example of a NAD501 log report.

```
NAD501 X.25 call terminated from OS, X.121 addr ‘A123456’.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<X.121 address>	Alphanumeric	Address of an operations support system

Action

None

—end—

NAD605

Report explanation

This log report confirms that an exerciser command was sent to the NE with no errors.

Report severity

Warning

Report format

The following is the format for a NAD605 log report.

NAD605 A request to <operation> the exerciser at NE <ne id> has been completed.

Report example

The following is a typical example of a NAD605 log report.

```
NAD605 A request to invoke the exerciser at NE 4807 has been
completed.
```

Field descriptions

The following table explains the variable field in the log report.

Field	**Value**	**Description**
<operation>	Character string: Schedule Invoke	Indicates the issued command
<ne id>	Numeric: 1-32767	Indicates the terminating network element number

Action

None

—end—

NAD606

Report explanation

This log report confirms that a switch command was sent to the NE with no errors.

Report severity

Warning

Report format

The following is the format for a NAD606 log report.

NAD606 A request to <operation> a <switch type> switch at NE <ne id> CPG <CPG> has been completed.

Report example

The following is a typical example of a NAD606 log report.

```
NAD606 A request to operate a forced switch at NE 4807 CPG G2
has been completed.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<operation>	Character string: Operate Release	Indicates the switch operation
<switch type>	Character string: Forced Manual Protection Lockout working	Indicates the switch type
<ne id>	Numeric: 1-32767	Indicates the terminating network element number
<CPG>	Alphanumeric: G1 or G2	Indicates the circuit pack group number

Action

None

—end—

NAD613

Report explanation

This log report indicates that a previous data inconsistency in protection data has been corrected.

Report severity

Warning

Report format

The following is the format for a NAD613 log report.

1:N protect data now consistent between NE <ne identifier> and OPC.

Report example

The following is a typical example of a NAD613 log report.

```
NAD613  1:N protect data now consistent between NE 43 and OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element

Action

None

—end—

NAD620

Report explanation

This log report indicates the successful completion of a scheduled audit of connection data in all NEs managed by this OPC. No data inconsistencies were found.

Report severity

Warning

Report example

The following is a typical example of a NAD620 log report.

```
NAD620 Audited Connections.
Result: Success.
The scheduled connection data audit found no inconsistent
connection data.
```

Action

No action required. This log confirms that the successful completion of the audit of OPC connection data against NE connection data.

—end—

NAD621

Report explanation

This log report indicates the successful completion of an Add Connection operation by the STS Connection Manager. STS-1 connection data has been updated at the OPC and the required action has been completed at the NEs.

Report severity

Warning

Report format

The following is the format for a NAD621 log report.

NAD621 Added STS-1 Connection.
Result: <result>
Connection Id: "<connection id>"
End NE A: "<ne id and name>"; End NE Z: "<ne id and name>"
Request initiated by user "<userid>".

Report example

The following is a typical example of a NAD621 log report.

```
NAD621 Added STS-1 Connection.
Result: Create and distribution successful.
Connection Id: "Main St King St 001"
End NE A: "2 MAIN"; End NE Z: "5 KING"
Request initiated by user "admin".
```

—continued—

NAD621, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<result>		Indicates the results of the operation taken by the system on behalf of the user to complete the provisioning request.
	Create and distribution successful	In this case, the STS-1 connection was added to the OPC connection inventory. This connection information was also distributed to those NEs, which pass through or add/drop this connection, to complete the provisioning request.
	Create successful	In this case, the STS-1 connection was added to the OPC connection inventory. No distribution was required since no NEs in this span of control were affected.
	Retry distribution successful	In this case, an attempt to retry updating affected NEs immediately following a failed connection distribution has succeeded at all affected NEs managed by this OPC.
<connection id>	String	The STS-1 Connection Identifier assigned by the user.
<ne id and name>	String	The network element number and name of the terminating network element.
<userid>	String	The user account name of the OPC user who requested this operation.

Action

None

—end—

NAD622

Report explanation

This log report indicates the successful completion of an Edit Connection operation by the STS Connection Manager. STS-1 connection data has been updated at the OPC and the required action has been completed at the NEs.

Report severity

Warning

Report format

The following is the format for a NAD621 log report.

NAD622 Edited STS-1 Connection.
Result: <result>
Connection Id: "<connection id>"
End NE A: "<ne id and name>"; End NE Z: "<neid and name>"
Request initiated by user "<userid>".

Report example

The following is a typical example of a NAD622 log report.

```
NAD622 Added STS-1 Connection.
Result: Success.
Connection Id: "Main St King St 001"
End NE A: "2 MAIN"; End NE Z: "5 KING"
Request initiated by user "admin".
```

—continued—

NAD622, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<result>		Indicates the results of the operation taken by the system on behalf of the user to complete the provisioning request.
	Create and distribution successful	In this case, the STS-1 connection was added to the OPC connection inventory. This connection information was also distributed to those NEs, which pass through or add/drop this connection, to complete the provisioning request.
	Create successful	In this case, the STS-1 connection was added to the OPC connection inventory. No distribution was required since no NEs in this span of control were affected.
	Retry distribution successful	In this case, an attempt to retry updating affected NEs immediately following a failed connection distribution has succeeded at all affected NEs managed by this OPC.
<connection id>	String	The STS-1 Connection Identifier assigned by the user.
<ne id and name>	String	The network element number and name of the terminating network element.
<userid>	String	The user account name of the OPC user who requested this operation.

Action

None

—end—

NAD623

Report explanation

This log report indicates the successful completion of a Delete Connection operation by the STS Connection Manager. STS-1 connection data has been updated at the OPC and the required action has been completed at the NEs.

Report severity

Warning

Report format

The following is the format for a NAD623 log report.

NAD623 Deleted STS-1 Connection.
Result: <result>
Connection Id: “<connection id>”
End NE A: "<ne id and name>"; End NE Z: "<ne id and name>"
Request initiated by user "<userid>".

Report example

The following is a typical example of a NAD623 log report.

```
NAD623 Deleted STS-1 Connection.
Result: Success.
Connection Id: "Main St King St 001"
End NE A: "2 MAIN"; End NE Z: "5 KING"
Request initiated by user "admin".
```

—continued—

NAD623, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<result>		Indicates the results of the operation taken by the system on behalf of the user to complete the provisioning request.
	Create and distribution successful	In this case, the STS-1 connection was added to the OPC connection inventory. This connection information was also distributed to those NEs, which pass through or add/drop this connection, to complete the provisioning request.
	Create successful	In this case, the STS-1 connection was added to the OPC connection inventory. No distribution was required since no NEs in this span of control were affected.
	Retry distribution successful	In this case, an attempt to retry updating affected NEs immediately following a failed connection distribution has succeeded at all affected NEs managed by this OPC.
<connection id>	String	The STS-1 Connection Identifier assigned by the user.
<ne id and name>	String	The network element number and name of the terminating network element.
<userid>	String	The user account name of the OPC user who requested this operation.

Action

None

—end—

NAD624

Report explanation

This log report indicates the successful completion of a scheduled audit of STS-1 connection data in all NEs managed by this OPC. No data inconsistencies were found.

Report severity

Warning

Report example

The following is a typical example of a NAD624 log report.

```
NAD624 Audited STS-1 Connections.
Result: Success.
The scheduled STS-1 connection data audit found no inconsistent
connection data.
```

Action

No action required. This log confirms that the audit is running correctly, at the scheduled time and frequency.

—end—

NAD625

Report explanation

This log report indicates the successful completion of a user initiated audit of STS-1 connection data. Any previous data inconsistencies between the OPC and NEs have been corrected.

Report severity

Warning

Report example

The following is a typical example of a NAD625 log report.

```
NAD625 Correct STS-1 Connections.
Result: Success.
STS-1 connection data has been corrected at NE(s) <ne list> with
the OPC’s view.
```

Field descriptions

The following table explains the variable field in this log report.

Field	Value	Description
<ne list>	Decimal number	Network element identifier

Action

None

—end—

NAD626

Report explanation

This log report is generated when STS-1 Connection Services have been successfully enabled for an AccessNode Point-to-Point configuration.

Report severity

Warning

Report format

The following is the format for a NAD626 log report.

NAD626 Enable STS-1 Connection Services action completed successfully for configuration with endpoints at NE A: <FCOT ne id> and
NE Z: <RFT ne id>.

Report example

The following is a typical example of a NAD626 log report.

```
NAD626 Enable STS-1 Connection Services action
completed successfully for configuration with endpoints
at NE A:1001 and NE Z:1002.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<FCOT ne id>	1-32767 (in OPC’s span of control)	NE id of FCOT in a point-to-point configuration for which STS-1 Connection Services has been enabled.
<RFTne id>	1-32767 (in OPC’s span of control)	NE id of RFT in a point-to-point configuration for which STS-1 Connection Services has been enabled.

Action

None

—end—

NAD630

Report explanation

When a user password is assigned in the OPC, it is automatically propagated to all network elements to which the user has been given access. This log is produced for each of those network elements.

Report severity

Warning

Report format

The following is the format for a NAD630 log report.

User <user identifier> assigned password on NE <ne identifier>.

Report example

The following is a typical example of a NAD630 log report.

```
NAD630 User Fred assigned password on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

None

—end—

NAD631

Report explanation

This log report indicates that the specified user’s password is disabled on all network elements to which the user has been given access.

Report severity

Warning

Report format

The following is the format for a NAD631 log report.

<user identifier>’s password disabled on NE <ne identifier>.

Report example

The following is a typical example of a NAD631 log report.

```
NAD631 Fred’s password disabled on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

None

—end—

NAD632

Report explanation

This log report indicates that permission to access the specified network element by the specified user has been revoked. This does not mean that the user account has been deleted from the OPC or that access permissions to other network elements have been revoked.

Report severity

Warning

Report format

The following is the format for a NAD632 log report.

User <user identifier> deleted from NE <ne identifier>.

Report example

The following is a typical example of a NAD632 log report.

```
NAD632 User Fred deleted from NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

None

—end—

NAD633

Report explanation

This log report indicates that specified user’s command class has been changed on the specified network element. The user’s command class refers to the capability of the user to view or modify data on the specified network element. The user’s command class on one network element is independent of the user’s command class on other network elements.

Report severity

Warning

Report format

The following is the format for a NAD633 log report.

<user identifier>’s command class updated on NE <ne identifier>.

Report example

The following is a typical example of a NAD633 log report.

```
NAD633 Fred’s command class updated on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

None

—end—

NAD634

Report explanation

This log indicates that the specified user has been given access to the specified network element. It does not necessarily indicate a new user account on the OPC.

Report severity

Warning

Report format

The following is the format for a NAD634 log report.

User <user identifier> created on NE <ne identifier>.

Report example

The following is a typical example of a NAD634 log report.

```
NAD634 User Fred created on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

None

—end—

NAD635

Report explanation

When a user password is changed in the OPC, either by an administrator or by the user, it is automatically propagated to all network elements to which the user has been given access. This log is produced for each of those network elements.

Report severity

Warning

Report format

The following is the format for a NAD635 log report.

<user identifier>’s password updated on NE <ne identifier>.

Report example

The following is a typical example of a NAD635 log report.

```
NAD635 Fred’s password updated on NE 43.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Serial number of the network element
<user identifier>	Text	A user account name

Action

None

—end—

NAD636

Report explanation

When a user password is assigned in the OPC, it is automatically propagated to all network elements to which the user has been given access. This log is produced to confirm password assignment on the OPC. Associated NAD630 log reports provide confirmation of password assignment for each network element to which the user has access.

Report severity

Warning

Report format

The following is the format for a NAD636 log report.

<user identifier> assigned password on OPC.

Report example

The following is a typical example of a NAD636 log report.

```
NAD636 User Fred assigned password on OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user identifier>	Text	A user account name

Action

None

—end—

NAD637

Report explanation

This log report indicates that the specified user password is disabled on the OPC. Associated NAD631 log reports provide confirmation of password disable for each network element to which the user has access.

Report severity

Warning

Report format

The following is the format for a NAD637 log report.

<user identifier>’s password disabled on OPC.

Report example

The following is a typical example of a NAD637 log report.

```
NAD637 Fred’s password disabled on OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user identifier>	Text	A user account name

Action

None

—end—

NAD638

Report explanation

This log report indicates that a user account has been deleted from the OPC. As a consequence, the account has been deleted in all network elements.

Report severity

Warning

Report format

The following is the format for a NAD638 log report.

<user identifier> delete from OPC.

Report example

The following is a typical example of a NAD638 log report.

```
NAD638 User Fred deleted from OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user identifier>	Text	A user account name

Action

None

—end—

NAD639

Report explanation

This log report indicates that a new user account has been created on the OPC. This does not mean that the user account can be used to log into the network elements. Associated log reports of type NAD634 will indicate accessibility to network elements.

Report severity

Warning

Report format

The following is the format for a NAD639 log report.

User <user identifier> created on OPC.

Report example

The following is a typical example of a NAD639 log report.

```
NAD639 User Fred created on OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user identifier>	Text	A user account name

Action

None

—end—

NAD640

Report explanation

When a user password is changed in the OPC, either by an administrator or by the user, it is automatically propagated to all network elements to which the user has been given access. This log is produced to confirm the change on the OPC. Associated NAD635 log reports will confirm the password change in affected network elements.

Report severity

Warning

Report format

The following is the format for a NAD640 log report.

<user identifier>’s password updated on OPC.

Report example

The following is a typical example of a NAD640 log report.

```
NAD640 Fred’s password updated on OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<user identifier>	Text	A user account name

Action

None

—end—

NAD700

Report explanation

This log report is generated when the user initiates the enabling of STS-1 Connection Services for an AccessNode Point-to-Point configuration using the Commission NE Connectivity dialog in the Commissioning Manager tool.

Report severity

Warning

Report format

The following is the format for a NAD700 log report.

NAD700 Enable STS-1 Connection Services action in progress for configuration with endpoints at NE A: <FCOT ne id> and
NE Z: <RFT ne id>.

Report example

The following is a typical example of a NAD700 log report.

```
NAD700 Enable STS-1 Connection Services action
completed successfully for configuration with endpoints
at NE A:1001 and NE Z:1002.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<FCOT ne id>	1-32767 (in OPC’s span of control)	NE id of FCOT in a point-to-point configuration for which STS-1 Connection Services is being enabled.
<RFT ne id>	1-32767 (in OPC’s span of control)	NE id of RFT in a point-to-point configuration for which STS-1 Connection Services is being enabled.

Action

None

—end—

NAD710

Report explanation

This log report confirms the new destination of network telemetry.

Report severity

Warning

Report format

The following is the format for a NAD710 log report.

Network telemetry will be sent to recommissioned NE <ne identifier>.

Report example

The following is a typical example of a NAD710 log report.

```
NAD710 Network telemetry will be sent to recommissioned NE 43.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Network element identifier

Action

None

—end—

NAD711

Report explanation

This log report indicates the identity of the network element which is collecting network telemetry, after a change in the assignment of telemetry to the network element occurs.

Report severity

Warning

Report format

The following is the format for a NAD711 log report.

NE <ne identifier> is the configured Remote Network Telemetry.

Report example

The following is a typical example of a NAD711 log report.

```
NAD711 NE 43 is the configured Remote Network Telemetry.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne identifier>	Decimal number	Network element identifier

Action

None

—end—

NAD730

Report explanation

This log report indicates that the system software upgrade has started.

Report severity

Warning

Report format

The following is the format for a NAD730 log report.

Upgrade starting of system software to < software release > as specified by the user in the Network Upgrade Manager.

Report example

The following is a typical example of a NAD730 log report.

```
Upgrade starting of system software to AN08 as specified by the
user in the Network Upgrade Manager.
```

Field descriptions

The following table explains the variable field in the log report.

Field	**Value**	**Description**
<software release>	Release number	Identifies software release.

Action

None

—end—

NAD731

Report explanation

This log report indicates that the system software upgrade has started.

Report severity

Warning

Report format

The following is the format for a NAD731 log report.

Starting upgrade to < software release > on network element < ne id >.

Report example

The following is a typical example of a NAD731 log report.

```
Starting upgrade to AN08 on network element 2.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne id>		Network element identifier.

Action

None

—end—

NE313

Report explanation

The network element (NE) failed to be provisioned.

Report format

The following is the format for the NE313 log report.

```
NE313 mmm:dd hh:mm:ss nnnn log_type log_label
Failed Operation: <operation>
Reason: <reason>
Network Id:          <nid>
System Id:           <sysid>
NE Id:               <neid>
```

Report example

The following shows a typical example of the NE313 log report.

```
NE313 MAR26 14:17:24 2100 TBL Operation Failed
Failed Operation: Create
Reason: Failed to create network element
Network Id:         1
System Id:          1
NE Id:              1
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<operation>	Create	Type of operation that failed
<reason>	Failed to create network element	Reason for the failure
<n1>	Integer	Network identifier
<n2>	Integer	System identifier
<n3>	Integer	Network element identifier

Action

Try to recreate the network element. For details, see *Commissioning and Testing*, Volume 3. If this fails, contact your next level of support.

—end—

NE401

Report explanation

This log notifies the craftsperson that the network element was created successfully.

Report format

The following is the format for the NE401 log report.

```
NE401 mmm:dd hh:mm:ss nnnn event_type event_label
Network Element successfully created
Network ID:                <nid>
System Id:                 <sysid>
NE Id:                      <neid>
```

Report example

The following shows a typical example of the NE401 log report.

```
NE401 MAR26 14:17:24 2100 INFO Create Success
Network Element successfully created
Network Id:          1
System Id:           1
NE Id:               1
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<nid>	Numeric	Network id
<sysid>	Numeric	System id
<ne id>	Numeric	Network element id

Action

None

—end—

NE402

Report explanation

This log notifies the craftsperson of the change made to an attribute of the network element.

Report format

The following is the format for log report NE402:

```
NE402 mmm:dd hh:mm:ss nnnn event_type event_label
Parameter Changed: <paramchgd>
Present: <pres>
Previous: <prev>
Network Id:          <nid>
System Id:           <sysid>
NE Id:               <neid>
```

Report example

The following shows a typical example of log report NE402:

```
NE402 MA26 14:17:24 2100 INFO Data Change
Parameter Changed: System Clock Source
Present: FreeRun
Previous: ExternalSync
Network Id:          1
System Id:           1
NE Id:               1
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<paramchgd>	Possible values are: System Clock Source NE Name	The NE attribute that was edited.
<pres>	Alphanumeric	Present value of the attribute

—continued—

—continued—

NE402, continued

Field	Value	Description
<prev>	For System Clock Source: FreeRun ExternalSync ThroughTimed LoopTimed LineTimed For NE Name: alphanumeric	Previous value of the attribute
<nid>	Numeric	Network id
<sysid>	Numeric	System id
<neid>	Numeric	Network element id
—end—		

Action

None

—end—

OPT301

Report explanation

This log reports a failure in the on/off procedure provided by an optional feature.

Report format

The following is the format for the OPT301 log report.

```
OPT301 mmm:dd hh:mm:ss nnnn event_type event_label
Feature Name:           <featname>
State:                  <state>
```

Report example

The following shows a typical example of the OPT301 log report.

```
OPT301 MAY12 12:34:56
Feature Name:        PARALLEL_TELEM
State:               OFF
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<featname>	Text string	Name of the optional feature package
<state>	ON, OFF	Current state of the optional feature

Action

Report to Field Support personnel.

If you want to view a list of the optional feature packages on your system, log in to a network element user interface and enter the following command at the CI level:

```
swkey ↵
dispipl ↵
```

A list of the optional feature packages appears.

—end—

OPT402

Report explanation

This log reports displays the reason that an allocation or deallocation operation failed.

Report format

The following is the format for the OPT402 log report.

```
OPT402 mmm:dd hh:mm:ss nnnn event_type event_label
Package Name:          <optional feature>
Operation Failed:      <allocation or deallocation>
Reason:                <failure reason>
```

Report example

The following shows a typical example of the OPT402 log report.

```
OPT402 MAY12 12:34:56
Package Name:        Bandwidth_Booster
Operation Failed:    Deallocation
Reason:              bandwidth_usage exceeds limitation
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<optional feature>	Bandwidth_Booster	Optional feature name
<allocation or deallocations>	Allocation or Deallocation	Operations for optional feature
<failure reason>	bandwidth_usage exceeds limitation	Reason for failure

Action

Access the FCOT UI to deactivate some DS1 or DS3 ports, query the bandwidth usage and then try to allocate the Bandwidth Booster option again from the OPC UI.

—end—

SCHD601

Report explanation

When the operation scheduler requested the execution of an operation, an error condition occurred preventing the execution of the request.

It is highly unlikely that this log will be generated for the Exerciser or the Backup (whose schedule is specified in the “Scheduler” screen). If it is, it means the system was too busy to process the request at the specified time. The operation will be requested again, at its next scheduled time.

This log is more likely to be generated for the PM Report operation which is responsible for updating the PM screen every 10 seconds. For instance, if the logical association between the PM screen application and the NE is lost (check the COML logs), this log will be generated. It may also be generated shortly after a restart, if the last database backup occurred while a PM screen was active. In the case of PM Report, the scheduled operation is deleted when this log is generated, meaning that the PM screen updating stops.

Report format

The following is the format for log report SCHD601.

```
SCHD601 mmm:dd hh:mm:ss nnnn event_type event_label
        Operation: <operation>          Reason code: <code>
```

Report example

The following shows a typical example of log report SCHD601.

```
SCHD601 FEB11 16:41:51 0700 INFO Scheduled operation failed.
     Operation: PM Report     Reason code:10
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<operation>	Exerciser Backup PM Report	Type of scheduled operation that failed
<code>	Integer	Code identifying the failure reason.

—continued—

SCHD601, continued

Action

The action to be taken when this log is generated depends on the scheduled operation that failed:

- For the Backup operation, it may be worthwhile to perform a manual backup, especially if provisioning changes were made since the previous backup.
- For the Exerciser operation, you may want to manually run the exerciser.
- If the PM Report scheduled operation fail log occurs while you are in a PM screen, re-select the screen to resume the automatic 10 second updating.

—end—

SCHD602

Report explanation

When the operation scheduler requested the execution of the specified operation, a time out occurred because the system was extremely busy. See SCHD601 for more information.

Report format

The following is the format for log report SCHD602.

```
SCHD602 mmm:dd hh:mm:ss nnnn event_type event_label
     Operation:        <operation>
```

Report example

The following shows a typical example of log report SCHD602.

```
SCHD602 FEB11 16:41:51 0800 INFO Scheduled operation timed out
     Operation:      PM Report
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<operation>	Exerciser Backup PM Report	Type of scheduled operation that failed

Action

The action to be taken when this log is generated depends on the scheduled operation that failed:

- For the Backup operation, it may be worthwhile to perform a manual backup, especially if provisioning changes were made since the previous backup.
- For the Exerciser operation, you may want to manually run the exerciser.
- If the PM Report fail log occurs while you are in a PM screen, re-select the screen to resume the automatic 10 second updating.

—end—

SDA300

Report explanation

This log report indicates that an unidentified error occurred during commissioning.

Report severity

Major

Report format

The following is the format for an SDA300 log report.

SDA300 Unknown error caused <operation identifier> failure.

Report example

The following is a typical example of an SDA300 log report.

```
SDA300 Unknown error caused Clear commissioning failure.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<operation identifier>	Clear commissioning Commission new system Edit system data Commission new network element Edit network element Delete network element Apply commissioning changes Transfer data to Primary OPC Transfer data to Backup OPC Transfer data to SLAT OPC Backup Restore Commission new OPC Edit OPC Delete OPC Initializing user interface	

Action

Retry the operation which failed. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact your service representative.

—end—

SDA301

Report explanation

This log report indicates that the clear commissioning operation failed.

Report severity

Major

Report format

The following is the format for an SDA301 log report.

SDA301 <cause> caused Clear commissioning failure.

Report example

The following is a typical example of an SDA301 log report.

```
SDA301 Failure to read database caused Clear commissioning
failure.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<operation identifier>	Failure to IPC init Failure to MIB connect Failure to CCH register Failure to create confirm table Failure to IPC term Failure to CCH terminate Failure to MIB disconnect Failure to connect to DRM Failure to busy MSRs Failure to read database Failure to erase NEdbs, dsa1, dsa2, opcname, trans1, trans2, soc, osihosts	Operation that failed

Action

Retry the clear commissioning operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA302

Report explanation

This log report indicates that a failure occurred during the commissioning of a new system.

Report severity

Major

Report format

The following is the format for an SDA302 log report.

SDA302 <cause> caused Commission new system failure.

Report example

The following is a typical example of an SDA302 log report.

```
SDA302 Missing OPC name caused Commission new system failure.
```

—continued—

SDA302, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<cause>	Missing nwid, sysid, ncfid Missing OPC sw version Missing OPC name Missing net address Bad net address Failure to parse serial number Failure to get net address Failure to open osihosts Failure to open clone Failure to read osihosts Failure to write osihosts Failure to copy osihosts Missing attribute Nonexistent attribute Nonexistent argument Invalid object instance Invalid action Out of memory Out of resources Time out Missing object Missing reference object Invalid attribute Duplicate object Unknown action type	Failure that occurred

Action

Retry the commissioning operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA303

Report explanation

This log report indicates that a failure occurred during the editing of system data.

Report severity

Major

Report format

The following is the format for an SDA303 log report.

SDA303 <cause> caused Edit system data failure.

Report example

The following is a typical example of an SDA303 log report.

```
SDA303 Missing OPC name caused Edit system data failure.
```

—continued—

SDA303, continued

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Missing nwid, sysid, ncfid Missing OPC sw version Missing OPC name Missing net address Bad net address Failure to parse serial number Failure to get net address Failure to open osihosts Failure to open clone Failure to read osihosts Failure to write osihosts Failure to copy osihosts Missing attribute Nonexistent attribute Nonexistent argument Invalid object instance Invalid action Out of memory Out of resources Time out Missing object Missing reference object Invalid attribute Duplicate object Unknown action type	Failure that occurred

Action

Retry the system data editing operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA304

Report explanation

This log report indicates that a failure occurred during the commissioning of a new network element.

Report severity

Major

Report format

The following is the format for an SDA304 log report.

SDA304 <cause> caused Commission new network element failure.

Report example

The following is a typical example of an SDA304 log report.

```
SDA304 Duplicate object caused Commission new network element
failure.
```

—continued—

SDA304, continued

Field descriptions

The following table explains each of the variable fields in the log report

Field	Value	Description
<cause>	Missing sysid, neid, eqid, eqtype, shtype, shserno, shorigin, genrel Missing table data Missing NE in table Failure to delete NE from SOC Failure to add NE to SOC Failure to query NE in SOC Failure to open trans1, trans2 Failure to read trans1, trans2 Failure to write trans1, trans2 Failure to backup trans1 Wrong transaction type Missing attribute Nonexistent attribute Nonexistent argument Invalid argument Invalid object instance Invalid action Out of memory Out of resources Time out Missing object Missing reference object Invalid attribute Duplicate object Unknown action type	Failure that occurred

Action

Retry the network element commissioning operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA305

Report explanation

This log report indicates that a failure occurred during the editing of network element data.

Report severity

Major

Report format

The following is the format for an SDA305 log report.

SDA305 <cause> caused edit network element failure.

Report example

The following is a typical example of an SDA305 log report.

```
SDA305 Duplicate object caused edit network element failure.
```

—continued—

SDA305, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<cause>	Missing sysid, neid, eqid, eqtype, shtype, shserno, shorigin, genrel Missing table data Missing NE in table Failure to delete NE from SOC Failure to add NE to SOC Failure to query NE in SOC Failure to open trans1, trans2 Failure to read trans1, trans2 Failure to write trans1, trans2 Failure to backup trans1 Wrong transaction type Missing attribute Nonexistent attribute Nonexistent argument Invalid argument Invalid object instance Invalid action Out of memory Out of resources Time out Missing object Missing reference object Invalid attribute Duplicate object Unknown action type	Failure that occurred

Action

Retry the network element editing operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA306

Report explanation

This log report indicates that a failure occurred during the deletion of a network element.

Report severity

Major

Report format

The following is the format for an SDA306 log report.

SDA306 <cause> caused delete network element failure.

Report example

The following is a typical example of an SDA306 log report.

```
SDA306 Duplicate object caused delete network element failure.
```

—continued—

SDA306, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<cause>	Missing sysid, neid, eqid, eqtype, shtype, shserno, shorigin, genrel Missing table data Missing NE in table Failure to delete NE from SOC Failure to add NE to SOC Failure to query NE in SOC Failure to open trans1, trans2 Failure to read trans1, trans2 Failure to write trans1, trans2 Failure to backup trans1 Wrong transaction type Missing attribute Nonexistent attribute Nonexistent argument Invalid argument Invalid object instance Invalid action Out of memory Out of resources Time out Missing object Missing reference object Invalid attribute Duplicate object Unknown action type	Failure that occurred

Action

Retry the network element delete operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA307

Report explanation

This log report indicates that a failure occurred during the application of commissioning changes.

Report severity

Major

Report format

The following is the format for an SDA307 log report.

SDA307 <cause> caused Apply commissioning changes failure.

Report example

The following is a typical example of an SDA307 log report.

```
SDA307 Duplicate object caused Apply commissioning changes
failure.
```

—continued—

SDA307, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<cause>	Missing sysid, neid, eqid, eqtype, shtype, shserno, shorigin, genrel Missing table data Missing NE in table Failure to delete NE from SOC Failure to add NE to SOC Failure to query NE in SOC Failure to open trans1, trans2 Failure to read trans1, trans2 Failure to write trans1, trans2 Failure to backup trans1 Wrong transaction type Missing attribute Nonexistent attribute Nonexistent argument Invalid argument Invalid object instance Invalid action Out of memory Out of resources Time out Missing object Missing reference object Invalid attribute Duplicate object Unknown action type	Failure that occurred

Action

Retry the commissioning application operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA308

Report explanation

This log report indicates that a failure occurred during the transfer of data from the portable OPC to the Primary OPC, during commissioning.

Report severity

Major

Report format

The following is the format for an SDA308 log report.

SDA308 <cause> caused Transfer data to Primary OPC failure.

Report example

The following is a typical example of an SDA308 log report.

```
SDA308 Bad source address caused Transfer data to Primary OPC
failure.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Bad source address Bad destination address Bad Env variable Time out Corrupt result file Error deleting result file Inactive local OPC Unrecognized error Fatal error	Failure that occurred

Action

Retry the data transfer operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA309

Report explanation

This log report indicates that a failure occurred during the transfer of data from the Primary OPC to the Backup OPC, during commissioning.

Report severity

Major

Report format

The following is the format for an SDA309 log report.

SDA309 <cause> caused Transfer data to Backup OPC failure.

Report example

The following is a typical example of an SDA309 log report.

```
SDA309 Bad source address caused Transfer data to Backup OPC
failure.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Bad source address Bad destination address Bad Env variable Time out Corrupt result file Error deleting result file Inactive local OPC Unrecognized error Fatal error	Failure that occurred

Action

Retry the data transfer operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA310

Report explanation

This log report indicates that a failure occurred during the transfer of data to the Portable OPC, during commissioning.

Report severity

Major

Report format

The following is the format for an SDA310 log report.

SDA310 <cause> caused Transfer data to SLAT OPC failure.

Report example

The following is a typical example of an SDA310 log report.

```
SDA310 Bad source address caused Transfer data to SLAT OPC
failure.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Bad source address Bad destination address Bad Env variable Time out Corrupt result file Error deleting result file Inactive local OPC Unrecognized error Fatal error	Failure that occurred

Action

Retry the data transfer operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA311

Report explanation

This log report indicates that a failure occurred during a data backup.

Report severity

Major

Report format

The following is the format for an SDA311 log report.

SDA311 <cause> caused Backup failure.

Report example

The following is a typical example of an SDA311 log report.

```
SDA311 Failure to archive database caused Backup failure.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Failure to IPC init Failure to MIB connect Failure to CCH register Failure to create confirm table Failure to IPC term Failure to CCH terminate Failure to MIB disconnect Failure to connect to DRM Failure to busy MSRs Failure to rts MSRs Failure to archive database Tape driver missing Unknown tape error Tar to tape Failure to backup OPCDB, opcname, trans1, soc,osihosts	Failure that occurred

Action

Retry the data backup operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA312

Report explanation

This log report indicates that a failure occurred during a data restoration.

Report severity

Major

Report format

The following is the format for an SDA312 log report.

SDA312 <cause> caused Restore failure.

Report example

The following is a typical example of an SDA312 log report.

```
SDA312 Failure to restore database caused Restore failure.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Failure to IPC init Failure to MIB connect Failure to CCH register Failure to create confirm table Failure to IPC term Failure to CCH terminate Failure to MIB disconnect Failure to connect to DRM Failure to busy MSRs Failure to rts MSRs Failure to restore database Tape driver missing Unknown tape error Tar from tape Failure to restore OPCDB, opcname, trans1, soc,osihosts	Failure that occurred

Action

Retry the data restore operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA313

Report explanation

This log report indicates that a failure occurred during the commissioning of a new OPC.

Report severity

Major

Report format

The following is the format for an SDA313 log report.

SDA313 <cause> caused commission new OPC failure.

Report example

The following is a typical example of an SDA313 log report.

```
SDA313 Missing OPC name caused commission new OPC failure.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Missing OPC name Missing net address Bad net address Failure to parse serial number Failure to get net address Failure to open osihosts Failure to open clone Failure to read osihosts Failure to write osihosts Failure to copy osihosts	Failure that occurred

Action

Retry the OPC commissioning operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA314

Report explanation

This log report indicates that a failure occurred during the editing of OPC data.

Report severity

Major

Report format

The following is the format for an SDA314 log report.

SDA314 <cause> caused edit OPC failure.

Report example

The following is a typical example of an SDA314 log report.

```
SDA314 Missing OPC name caused edit OPC failure.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<cause>	Missing OPC name Missing net address Bad net address Failure to parse serial number Failure to get net address Failure to open osihosts Failure to open clone Failure to read osihosts Failure to write osihosts Failure to copy osihosts	Failure that occurred

Action

Retry the edit OPC operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA315

Report explanation

This log report indicates that a failure occurred during the deletion of an OPC.

Report severity

Major

Report format

The following is the format for an SDA315 log report.

SDA315 <cause> caused delete OPC failure.

Report example

The following is a typical example of an SDA315 log report.

```
SDA315 Missing OPC name caused delete OPC failure.
```

Field descriptions

The following table explains each of the variable fields in the log report

Field	Value	Description
<cause>	Missing OPC name Missing net address Bad net address Failure to parse serial number Failure to get net address Failure to open osihosts Failure to open clone Failure to read osihosts Failure to write osihosts Failure to copy osihosts	Failure that occurred

Action

Retry the OPC delete operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA316

Report explanation

This log report indicates that a failure occurred during the initialization of the user interface.

Report severity

Major

Report format

The following is the format for an SDA316 log report.

SDA316 <cause> caused failure in initializing user interface.

Report example

The following is a typical example of an SDA316 log report.

```
SDA316 Failure to initiate help caused failure in initializing
user interface.
```

—continued—

SDA316, continued

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<cause>	Failure to initiate help Failure to IPC init Failure to MIB connect Failure to CCH register Failure to create confirm table Failure to register with DRM Inactive OPC Missing nwid, sysid, ncfid Missing OPC sw version Missing OPC name Missing net address Bad net address Failure to parse serial number Failure to get net address Failure to open osihosts Failure to open clone Failure to read osihosts Failure to write osihosts Failure to copy osihosts Missing attribute Nonexistent attribute Nonexistent argument Invalid object instance Invalid action Out of memory Out of resources Time out Missing object Missing reference object Invalid attribute Duplicate object Unknown action type	Failure that occurred

Action

Retry the user interface initialization operation. If the same error occurs, shut down the OPC and retry the operation after the OPC reboots. If this fails, contact Nortel Networks support and report the cause which is indicated in the log report.

—end—

SDA320

Report explanation

This log report indicates that a software package on the OPC or NE has not been enabled or disabled successfully.

Report severity

Warning

Report format

The following is the format for an SDA320 log report.

SDA320 <customer personality file id> package <feature id> not <operation> on <equipment type> <ne id >; <reason>

Report example

The following are typical examples of an SDA320 log report.

```
SDA320 CPF package NTX0099 not enabled on NE 12345; the package
is not compatible with EQ type.
```

```
SDA320 Audit package NTX0100 not enabled on OPC; a request for
a duplicate allocations was made.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<customer personality field>	CPF, Manual, or Audit	Identifies the initiator of the action
<feature id>	Text of 12 characters	Engineering code
<operation>	Enabled or disabled	Action performed on the feature id
<equipment type>	NE or OPC	Equipment type
<ne id >	Decimal number	Identification of the equipment on which the package resides. This value is added for the NE only.
<reason>	Text	Reason for the failure

—continued—

SDA320, continued

Action

The required action depends on the reason for the failure:

If a memory error occurred at the NE, the network element has a serious problem with memory. Call Nortel Networks support.

If the tokens are currently in use, log in to the network element and deprovision the package. Restart your operation from the Software Optionality Management User Interface.

If the package is not compatible with the EQ type, the package is not available on this equipment type. No action is required.

If a request for a duplicate allocation was made, the NE has the software option in the same state as the request. The OPC will correct this situation. No action is required.

If the package could not be found, call Nortel Networks support to verify the possible mismatch of package name between the OPC and NE.

If there was an unknown error that occurred, login in to the NE and look at the OPT logs. Contact Nortel Networks support and report the problem.

If the allocation request exceeds the maximum allowable tokens for this package, redo the operation with a number less than the current number. (The NE hardware has a maximum number of allowable tokens.)

If the communication failed, the message could not be sent. Redo your operation after the association to that NE is up. Refer to COM502 for required action.

If a memory shortage occurred at the OPC, contact Nortel Networks support to investigate the problem.

If a system error occurred, contact Nortel Networks support to investigate the problem.

If a mismatch NTX code between the OPC and NE occurred, the audit will straighten this out. No action is required.

—end—

SDA326

Report explanation

This log report indicates that the maximum disk space allocated for NE loads would have been exceeded in the specific OPC, during the current network upgrade. The upgrade process has been suspended at the indicated step.

Report severity

Warning

Report format

The following is the format for an SDA326 log report.

SDA326 Network upgrade failed in step <upgrade step>. NE load limit of <load limit> kB will be exceeded on the <opc type> OPC. Delete unused NE loads on the <opc type> OPC and restart the upgrade.

Report example

The following is a typical example of an SDA326 log report.

```
SDA326 Network upgrade failed in step 7. NE load limit of 250
kB will be exceeded on the primary OPC. Delete unused NE loads
on the primary OPC and restart the upgrade.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<upgrade step>	Decimal number	Step number of the network upgrade method of procedure (MOP)
<load limit>	Decimal number	Number of kBytes allocated for network element software loads
<opc type>	Primary or backup	Type of OPC

—continued—

SDA326, continued

Action

If there are too many NE loads on the primary OPC, delete some NE loads using the procedure describing how to delete a software load from the primary OPC in the upgrade MOP. Once the NE loads have been removed, restart the upgrade from the beginning of the indicated upgrade step.

If there are too many NE loads on the backup OPC, delete some NE loads using the procedure describing how to delete a software load from the backup OPC in the upgrade MOP. Once the NE loads have been removed, restart the upgrade from the beginning of the indicated upgrade step.

—end—

SDA327

Report explanation

This log report indicates that during the network upgrade there was not enough space on the disk on the indicated OPC to accommodate the new NE software loads or the OPC software load. The upgrade process has been suspended.

Report severity

Warning

Report format

The following is the format for an SDA327 log report.

SDA327 Network upgrade failed in step <upgrade step>. <space shortage> kB of disk space need to be freed on the <opc name> OPC. Free the disk space and restart the upgrade.

Report example

The following is a typical example of an SDA327 log report.

```
SDA327 Network upgrade failed in step 27. 57 kB of disk space
need to be freed on the primary OPC. Free the disk space and
restart the upgrade.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<upgrade step>	Decimal number	Step number of the network upgrade change application procedure (CAP)
<space shortage>	Decimal number	Number of kBytes of OPC disk space required to continue the upgrade
<opc type>	Primary or backup	Type of OPC

Action

Contact Nortel Networks support as outlined in *Alarm and Trouble Clearing Procedures,* 323-3001-543, in *Maintenance*, Volume 5A, for assistance in determining what to delete. Then, resume the upgrade.

—end—

SDA328

Report explanation

This log report indicates that the current release of OPC software is not supported by the upgrade procedure that is being used.

Report severity

Warning

Report format

The following is the format for an SDA328 log report.

SDA328 Wrong upgrade procedure for software release. Contact Northern Telecom for the correct procedure.

Report example

The following is a typical example of an SDA328 log report.

```
SDA328 Wrong upgrade procedure for software release. Contact
Northern Telecom for the correct procedure.
```

Action

Contact Nortel Networks support as outlined in *Alarm and Trouble Clearing Procedures,* 323-3001-543, in *Maintenance*, Volume 5A, to determine the correct upgrade procedure to use for that software release.

—end—

SDA329

Report explanation

This log report indicates that the network upgrade has failed. If there is a specific reason for the failure it will be given.

Report severity

Warning

Report format

The following is the format for an SDA329 log report.

SDA329 Network upgrade failed in step <upgrade step>. <reason>.

Report example

The following is a typical example of an SDA329 log report.

```
SDA329 Network upgrade failed in step 33.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<upgrade step>	Decimal number	Step number of the network upgrade change application procedure (CAP)
<reason>	String	Cause of the failure (if available)

Action

Diagnose the problem based on the reason supplied in the log. If the reason for the failure is not apparent from the log, contact your Nortel Networks service representative, as outlined in *Alarm and Trouble Clearing Procedures*, 323-3001-543 in *Maintenance*, Volume 5A. Then, correct the source of the problem and resume the upgrade.

—end—

SDA330

Report explanation

This log report indicates that the specified NE’s were unable to perform database backups to the primary OPC, as requested by the network software upgrade. The upgrade has been suspended.

Report severity

Warning

Report format

The following is the format for an SDA330 log report.

SDA330 Network to force NE database backups for: <ne string>. The indicated NEs have failed to send a database backup to the primary OPC as requested by the network software upgrade.

Report example

The following is a typical example of an SDA330 log report.

```
SDA330 Network to force NE database backups for: NEs 1, 2 and
7. The indicated NEs have failed to send a database backup to
the primary OPC as requested by the network software upgrade.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<ne string>	Set of decimal numbers	Set of network element identifiers

Action

Using the Event Browser tool, verify that all NEs have association with the backup or the primary OPC and then restart the upgrade procedure. Verify that there is physical connectivity between the OPC and the NEs. Check for related logs in the event browser. Act on any information obtained.

If this fails, contact Nortel Networks support.

—end—

SDA331

Report explanation

This log report indicates that a data synchronization between the primary and backup OPCs could not be completed during a network upgrade. A transfer must be done to ensure that the NE database backups on the backup OPC are identical to those on the primary.

Report severity

Warning

Report format

The following is the format for an SDA331 log report.

SDA331 failed to force the data to be transferred from the primary OPC to the backup OPC as requested by the network upgrade software. <reason>.

Report example

The following is a typical example of an SDA331 log report.

```
SDA331 Failed to force the data to be transferred from the
primary OPC to the backup OPC as requested by the network
upgrade software. Communication error.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<reason>	String	Reason for failure

Action

Resolve the problem identified in the reason portion of the log. Then, restart the upgrade.

—end—

SDA332

Report explanation

This log report indicates that a network upgrade cannot continue, for the reason given.

Report severity

Warning

Report format

The following is the format for an SDA332 log report.

SDA332 This system has failed pre-upgrade validations. The user can not proceed with the network upgrade until the following problem is resolved: <reason>.

Report example

The following is a typical example of an SDA332 log report.

```
SDA330 This system has failed pre-upgrade validations. The user
can not proceed with the network upgrade until the following
problem is resolved: Local OPC is not an active Primary OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<reason>	Local OPC is not an active Primary OPC There is no Backup OPC commissioned or the Backup OPC is not in an “inactive” state The Primary OPC can not communicate with the Backup OPC	

—continued—

SDA332, continued

Action

If the reason field indicates Local OPC is not an active Primary OPC, check to make sure you are performing the upgrade on the primary OPC and it is active. Do this by using the OPC Status tool. If this is not the primary OPC, log out and run the upgrade procedure from the primary.

If you are performing the upgrade on the primary OPC and it is inactive, there is something wrong with it. Use the Event Browser to determine when and why the primary stopped being active. The OPC may have to be replaced.

If the reason field indicates There is no Backup OPC commissioned or the Backup OPC is not in an "inactive" state, use the commissioning manager to verify that there is a backup OPC commissioned. If there is no backup OPC commissioned, the upgrade can not be performed.

If there is a backup OPC commissioned, attempt to log on to the backup OPC as an admin-type user. If the backup is inactive, you will not be able to log in and the messages "This OPC is not active" and "Login has been disabled for this user" should appear.

If the backup OPC is active the login attempt should be successful, in which case use the Event Browser logs to determine when and why the backup OPC became active. If a "Critical Software Failure has occurred" message appears, then the backup OPC is non-functional. Contact Nortel Networks support.

If the reason field indicates The Primary OPC can not communicate with the Backup OPC, attempt to log in to the backup OPC. If the user can not connect to the backup OPC or does not obtain a login prompt, there is a physical connectivity problem. Ensure an end to end connection exists between the primary and backup OPCs. When the problem is corrected, restart the upgrade.

—end—

SDA337

Report explanation

This log report is generated when the system fails to meet the hardware baseline requirements during a software upgrade.

Report severity

Warning

Report format

The following is the format for an SDA337 log report.

SDA337 This system fails to meet the hardware baseline requirements for <release>.

Report example

The following is a typical example of an SDA337 log report.

```
SDA337 This system fails to meet the hardware baseline
requirements for ANrel10.00.
```

Field descriptions

The following table explains each of the variable field in the log report.

Field	Value	Description
<release>	Character string	The release name to which the system was being upgraded

Action

None

—end—

SDA340

Report explanation

This log report is generated when a communications problem occurs between the OPC and the remote host at <IP address>, and if the problem is not fixed within about 5 minutes. (The software delivery is then suspended for at least 20 minutes before any attempt is made to continue the software delivery from the point of failure.)

Report severity

Warning

Report format

The following is the format for an SDA340 log report.

SDA340 Electronic software delivery from <IP address> suspended.

Report example

The following is a typical example of an SDA340 log report.

```
SDA340 Electronic software delivery from 192.1.2.34 suspended.
```

Field descriptions

The following table explains each of the variable field in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release was being obtained

Action

None

—end—

SDA341

Report explanation

This log report is generated when the execution of a previously suspended software delivery is continued from the point of failure.

Report severity

Warning

Report format

The following is the format for an SDA341 log report.

SDA341 Electronic software delivery from <IP address> continued.

Report example

The following is a typical example of an SDA341 log report.

```
SDA341 Electronic software delivery from 192.1.2.34 continued.
```

Field descriptions

The following table explains each of the variable field in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release was being obtained

Action

None

—end—

SDA346

Report explanation

This log report indicates that a network element cannot establish a communications link with the OPC. This report appears when a network element tries to establish a link with the wrong OPC or when it tries to establish a link while it is already communicating with the correct OPC.

Report severity

Minor

Report format

The following is the format for an SDA346 log report.

SDA346 Unable to download to NE <ne id >; no suitable load found. Ensure that a software load for this <type identifier> shelf processor is installed in this OPC.

Report example

The following is a typical example of an SDA346 log report.

```
SDA346 Unable to download to NE 43; no suitable load found.
Ensure that a software load for this shelf processor is
installed in this OPC.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne id >	Decimal number	Serial number of the network element
<type identifier>	Unknown type of access	The processor type could not be determined AccessNode processor.

Action

Since no software load is available for this network element type, any network element which requires a software load will be unable to function. The required software load must be provided to the OPC as soon as possible.

—end—

SDA349

Report explanation

This log report indicates that an NE software load which should be available for downloading is not on the OPC. The software was not loaded successfully, or it has been deleted.

Report severity

Minor

Report format

The following is the format for an SDA349 log report.

SDA349 NE software load <load identifier> unavailable on OPC. Transfer it to OPC.

Report example

The following is a typical example of an SDA349 log report.

```
SDA349 NE software load TXP06CHIPL2 unavailable on OPC. Transfer
it to OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<load identifier>	Text	Identifies the load

Action

Reload into the OPC the NE software load specified in the log message.

—end—

SDA350

Report explanation

This log report indicates that a backup of OPC data has failed.

Report severity

Warning

Report format

The following is the format for an SDA350 log report.

SDA350 File backup to tape failed; <reason>.

Report example

The following is a typical example of an SDA350 log report.

```
SDA350 File backup to tape failed; disk is full.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<reason>	Transient error	Database was too busy to handle the file backup request.
	Disk is full	No disk space was available for the backup data.

Action

If the reason field indicates transient error, try the backup operation again.

If the reason field indicates disk is full, some disk space must be made available by the removal of files (such as previous backups).

—end—

SDA351

Report explanation

This log report indicates that a restoration of OPC data from tape has failed.

Report severity

Warning

Report format

The following is the format for an SDA351 log report.

SDA351 File restore from tape failed; <reason>.

Report example

The following is a typical example of an SDA351 log report.

```
SDA351 File restore from tape failed; defective tape.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<reason>	Transient error	Database was too busy to handle the file backup request
	Disk is full	No disk space was available for the backup data
	Defective tape	Tape cannot be used for this operation; the contents of this tape cannot be recovered.

Action

If the reason field indicates Transient error, try the backup operation again.

If the reason field indicates Disk is full, some disk space must be made available by the removal of files (such as previous backups).

If the reason field indicates Defective tape, use another backup tape.

—end—

SDA352

Report explanation

This log may indicate a commissioning error. If a valid serial number belonging to another NE is entered, the OPC will accept it, but it will be unable to respond to this network element's requests.

Report severity

Warning

Report format

The following is the format for an SDA352 log report.

SDA352 Unable to download to NE <ne id >; not in OPC's span of control. Commissioning of this <shelf type> shelf may have been performed incorrectly. Verify the serial number of this NE.

Report example

The following is a typical example of an SDA352 log report.

```
SDA352 Unable to download to NE 43; not in OPC's span of control.
Commissioning of this terminal shelf may have been performed
incorrectly. Verify the serial number of this NE.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne id >	Decimal number	Serial number of the network element
<shelf type>	Untyped access	Unknown shelf type

Action

Check to see that the serial number for the network element is correct by connecting a VT100 terminal to the NE and resetting the NE. During reset, the (partial) serial number is displayed momentarily on the VT100 screen.

—end—

SDA353

Report explanation

This log report indicates that software was not to be downloaded from the OPC to the specified network element, because the request received by the OPC from the network element contained an error.

Report severity

Minor

Report format

The following is the format for an SDA353 log report.

SDA353 Unable to download to NE <ne id >; invalid NE request format. If this problem persists, run diagnostics on this <shelf type> shelf and replace if necessary.

Report example

The following is a typical example of an SDA353 log report.

```
SDA353 Unable to download to NE 43; invalid NE request format.
If this problem persists, run diagnostics on this shelf and
replace if necessary.
```

Field descriptions

The following table explains each of the variable fields in the log report

Field	Value	Description
<ne id >	Decimal number	Serial number of the network element
<shelf type>	Untyped access	Unknown shelf type

Action

Software download will be retried automatically. If the cause was a communications error, the software download will be successful and no additional log will appear. However, if the problem persists, this log will appear at a frequency of about once every 30 seconds. In this case, the shelf processor sending the request may have failed. Run diagnostics on the shelf processor and replace if necessary.

—end—

SDA365

Report explanation

This log report indicates a defective tape. A transfer of NE software from this tape to the OPC was being attempted.

Report severity

Warning

Report format

The following is the format for an SDA365 log report.

SDA365 Unable to read NE software from tape to OPC; defective tape.
Transfer the contents of the previous NE software tape back again.

Action

Contact your Nortel Networks service representative for a replacement tape, containing the network element software load you are unable to read. Until you receive it, you must continue to run the existing network element software load.

—end—

SDA366

Report explanation

This log report indicates that network element software load files have been transferred successfully from tape to the OPC, but they are not available to the Reboot/Load Manager.

Report severity

Warning

Report format

The following is the format for an SDA366 log report.

SDA366 NE software transferred to OPC not available for distribution to NEs. At the command line, type ‘rafgo’.

Action

Log into the OPC as a user with access to the UNIX shell. Open the shell and type the command “rafgo” at the “OPC>” prompt. If you continue to receive these logs, contact your Nortel Networks service representative.

—end—

SDA367

Report explanation

This log report indicates that the network element software load that you are trying to transfer to the OPC is already on the OPC.

Report severity

Warning

Report format

The following is the format for an SDA367 log report.

SDA367 Failed to transfer NE software to OPC; this load already on OPC. If you still want to transfer it, first delete the existing load, then do the transfer.

Action

If you want to replace the current load, you must first delete the current load.

—end—

SDA369

Report explanation

This log report indicates that the specified software load that is being sent to the specified network element is not reaching its destination for the following reasons:

- The network element is not responding.
- The network element has been reset.
- The network element has aborted the download operation.

Report severity

Warning

Report format

The following is the format for an SDA369 log report.

SDA369 Unable to download <load identifier> to <ne id >; <reason>.

Report example

The following is a typical example of an SDA369 log report.

```
SDA369 Unable to download TXP06CHIPL2 to 43; NE aborted it.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<load identifier>	Text	NE software load name
<ne id >	Decimal number	Serial number of the network element
<reason>	NE is not responding NE has been reset NE aborted it	Reason for failed download

—continued—

SDA369, continued

Action

Step	Action
	Note: Software download will be retried automatically.
1	Check to make sure you are downloading the correct software to the processor. The ABM shelves must be equipped with the NT4K52FB, which is the 64 meg processor.
2	If the problem persists, run diagnostics on the shelf processor. There may be a problem with the shelf processor in the NE.

—end—

SDA379

Report explanation

This log report indicates that the installation of an OPC software load has failed.

Report severity

Major

Report format

The following is the format for an SDA379 log report.

SDA379 On <remote opc identifier>, failed to install <software release>.

Report example

The following is a typical example of an SDA379 log report.

```
SDA379 On opcm005, failed to install SX7E86AA0701.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<remote opc identifier>	Text	OPC name
<software release>	Text	Name of the software release

Action

Determine the cause of the failure by viewing the error messages in the Status Message area in the main window of the Remote OPC Installation tool, or by opening the View History dialog from the Utilities menu of that tool. Analyze the information found in these areas to identify the problem. Problems can be classified by the time required to repair them, as follows.

If you can fix the problem quickly, do so and then continue with the installation procedure on this OPC.

If you can fix the problem with additional time, and the problem does not affect the installation of software to other OPCs, install software to other OPCs. Then repair the problem and complete the software installation to the OPC which had the problem.

If you cannot fix the problem at this time, and it affects the installation of new software to all OPCs, re-install the previous software release.

—end—

SDA397

Report explanation

This log report indicates that the specified network element software load was successfully transferred between the two specified OPCs. However, the load could not be installed on network elements. There should be a corresponding log SDA703 which indicates the beginning of this transfer.

The cause of this failure is a corruption of data during the transfer, or an unknown error at the receiving OPC.

Report severity

Warning

Report format

The following is the format for an SDA397 log report.

SDA397 Install fail: file, <load identifier>, from <opc identifier> to <opc identifier>. The <operation type> file was successfully transferred but it could not be installed. The transfer was initiated from <opc identifier>.

Report example

The following is a typical example of an SDA397 log report.

```
SDA397 Transfer fail: file, TXP06CHIPL2, from opcm002 to
opcm003. The NE load file was successfully transferred but it
could not be installed. The transfer was initiated from opcm002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<load identifier>	Text	File name of the software load
<opc identifier>	Text	OPC name
<operation type>	NE load	Network element load

Action

Try the transfer again. If it fails the second time, look for logs indicating a problem on the receiving OPC.

—end—

SDA398

Report explanation

This log report indicates a failure to transfer the specified network element software load between the two specified OPCs. There should be a corresponding log SDA703 which indicates the beginning of this transfer.

Report severity

Warning

Report format

The following is the format for an SDA398 log report.

SDA398 Transfer fail: file, <load identifier>, from <opc identifier> to <opc identifier>. The <file type> transfer was initiated from <opc identifier>.

Report example

The following is a typical example of an SDA398 log report.

```
SDA398 Transfer fail: file, TXP06CHIPL2, from opcm002 to
opcm003. The NE load transfer was initiated from opcm002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<load identifier>	Text	File name of the software load
<opc identifier>	Text	OPC name
<operation type>	NE load	Network element load

Action

Try the transfer again. If it still fails, verify that the communications link between the OPCs is operating normally. If it is, try a different software delivery tape.

—end—

SDA500

Report explanation

This log report indicates that a package on the OPC or NE has been enabled or disabled successfully.

Report severity

Warning

Report format

The following is the format for an SDA500 log report.

SDA500 <customer personality file id> package <feature id> <operation> on <equipment type> <ne id >.

Report example

The following are typical examples of an SDA500 log report.

```
SDA500 CPF package NTX0099 enabled on NE 12345.
```

```
SDA500 Manual package NTX0100 enabled on OPC.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<customer personality field>	CPF, Manual, or Audit	Identify the initiator of the action which is Customer Personality File, UI command, or Audit.
<feature id>	Text of 12 characters	Engineering code.
<operation>	Enabled or disabled	Action performed on the feature id.
<equipment type>	NE or OPC	Equipment type.
<ne id >	Decimal number	Identification of the equipment on which the package resides. This value is added for the NE only.

Action

The Operating Company should disable the package if it is not bought. When the package is not purchased the “customer personality file id” field is set to NULL.

—end—

SDA506

Report explanation

This log report indicates that the value of the specified statistics counter has been reset to zero.

Report severity

Warning

Report format

The following is the format for an SDA506 log report.

SDA506 Stats count reset for ‘<counter identifier>’.

Report example

The following is a typical example of an SDA506 log report.

```
SDA506 Stats count reset for ‘total successful downloads’.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<counter identifier>	Successful downloads for processor Failed downloads for processor Total time for processor Total successful downloads Total requests received Total requests granted Total protocol data units transmitted Total protocol data units retransmitted	Type of statistic

Action

None

—end—

SDA510

Report explanation

This log report is generated when a client application submits a software release delivery.

Report severity

Warning

Report format

The following is the format for an SDA510 log report.

SDA510 Electronic software delivery <release name> submitted by user
<bftpd user ID> logged in from <bftpd client name>.
The software will be delivered <time>.
It will be obtained from IP host <IP address>.
The software will be transferred <rate>.

Report example

The following is a typical example of an SDA510 log report.

```
SDA510 Electronic software delivery of release AN12 submitted
by user admin logged in from Network Manager netman03
(192.1.2.34).
The software will be delivered at or after Wed Mar 15 01:00:00
1995.
It will be obtained from IP host 192.1.2.34.
The software will be transferred at the maximum rate of 1024
bytes per second.
```

—continued—

SDA510, continued

Field descriptions

The following table explains the variable fields in the log report.

Field	Value	Description
<release name>	Character string	The name of the software release to be delivered
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.
<time>	Character string	The time at which the software release will be delivered
<IP address>	Character string	The IP address of the host from which the software release will be obtained
<rate>	Character string	The maximum rate (in bytes per second) at which the software will be delivered from the remote IP host to the OPC

Action

None

—end—

SDA511

Report explanation

This log report is generated when a previously submitted software delivery command becomes active.

Report severity

Warning

Report format

The following is the format for an SDA511 log report.

SDA511 Electronic software delivery from <IP address> started.

Report example

The following is a typical example of an SDA511 log report.

```
SDA511 Electronic software delivery from 192.1.2.34 started.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained

Action

None

—end—

SDA512

Report explanation

This log report is generated after a software delivery command is successfully executed.

Report severity

Warning

Report format

The following is the format for an SDA512 log report.

SDA512 Electronic software delivery from <IP address> completed.

Report example

The following is a typical example of an SDA512 log report.

```
SDA512 Electronic software delivery from 192.1.2.34 completed.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained

Action

None

—end—

SDA513

Report explanation

This log report is generated when a previously submitted software delivery command is cancelled.

Report severity

Warning

Report format

The following is the format for an SDA513 log report.

SDA513 Electronic software delivery from <IP address> cancelled by user <bftpd user ID> logged in from <bftpd client name>.

Report example

The following is a typical example of an SDA513 log report.

```
SDA513 Electronic software delivery from 192.1.2.34 cancelled
by user admin logged in from Network Manager netman03
(192.1.2.34).
```

Field descriptions

The following table explains the variable fields in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.

Action

None

—end—

SDA514

Report explanation

This log report is generated when a previously submitted software delivery command is paused.

Report severity

Warning

Report format

The following is the format for an SDA514 log report.

SDA514 Electronic software delivery from <IP address> paused by user
<bftpd user ID> logged in from <bftpd client name>.
The pause will expire at or after <time>.

Report example

The following is a typical example of an SDA514 log report.

```
SDA514 Electronic software delivery from 192.1.2.34 cancelled
by user admin logged in from Network Manager netman03
(192.1.2.34).
The pause will expire at or after Wed Mar 15 14:00:00 1995.
```

—continued—

SDA514, continued

Field descriptions

The following table explains the variable fields in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.
<time>	Character string	The time at (or after) which the pause will expire

Action

None

—end—

SDA515

Report explanation

This log report is generated when a paused software delivery is paused again. This is usually done in order to extend the pause period.

Report severity

Warning

Report format

The following is the format for an SDA515 log report.

SDA515 Electronic software delivery from <IP address> paused by user
<bftpd user ID> logged in from <bftpd client name>.
The software delivery was already paused.
The pause will now expire at or after <time>.

Report example

The following is a typical example of an SDA515 log report.

```
SDA515 Electronic software delivery from 192.1.2.34 cancelled
by user admin logged in from Network Manager netman03
(192.1.2.34).
The software delivery was already paused.
The pause will now expire at or after Thur Mar 16 14:00:00 1995.
```

—continued—

SDA515, continued

Field descriptions

The following table explains the variable fields in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained.
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.
<time>	Character string	The time at (or after) which the pause will expire.

Action

None

—end—

SDA516

Report explanation

This log report is generated when a paused software delivery is resumed.

Report severity

Warning

Report format

The following is the format for an SDA516 log report.

SDA516 Electronic software delivery from <IP address> resumed by user <bftpd user ID> logged in from <bftpd client name>.

Report example

The following is a typical example of an SDA516 log report.

```
SDA516 Electronic software delivery from 192.1.2.34 resumed by
user admin logged in from Network Manager netman03 (192.1.2.34).
```

Field descriptions

The following table explains the variable fields in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained.
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.

Action

None

—end—

SDA517

Report explanation

This log report is generated when a previously submitted software delivery command is modified. Both the time at which the software will be delivered and the rate of transfer can be modified.

Report severity

Warning

Report format

The following is the format for an SDA517 log report.

SDA517 Electronic software delivery from <IP address> modified by user
<bftpd user ID> logged in from <bftpd client name>.
<changes>

Report example

The following is a typical example of an SDA517 log report.

```
SDA517 Electronic software delivery from 192.1.2.34 resumed by
user admin logged in from Network Manager netman03 (192.1.2.34).
The software will now be delivered as soon as possible.
The software will now be transferred as fast as possible.
```

—continued—

SDA517, continued

Field descriptions

The following table explains the variable fields in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained.
<bftpd user ID>	Character string	An OPC user ID, or if the client is logged in on behalf of a Network Manager user, a Network Manager user ID.
<bftpd client name>	Character string	Identifies the bftpd client. If the client is logged in on behalf of a Network Manager user, this field identifies the Network Manager's host name and IP address.
<changes>	Character string	The new value of the modified command parameters

Action

None

—end—

SDA518

Report explanation

This log report is generated when a software delivery command fails.

Report severity

Warning

Report format

The following is the format for an SDA518 log report.

SDA518 Electronic software delivery from <IP address> failed.
<reason>

Report example

The following is a typical example of an SDA518 log report.

```
SDA518 Electronic software delivery from 192.1.2.34 failed.
Pause timer expired.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<IP address>	Character string	The IP address of the host from which the software release will be obtained
<reason>	Character string	The reason why the software delivery failed

Action

If the reason is a corrupted file from the directory, try again. If you still get this message, the software release on the remote host is probably corrupted and should be replaced (by reloading the software release tape on the remote host). Otherwise, the health of the underlying IP network should be verified.

If the reason is the inability to find or access the file in a specific directory on a specific host with a specific user ID, ask the system administrator of the remote host to verify that the file actually exists in the directory, and that the user has read access on the file. If the file does not exist, the software release is corrupted and should be replaced. Otherwise, ask the system administrator of the remote host to grant the user access to the software release files.

—continued—

SDA518, continued

If the reason is the inability to find a valid software release in a directory on an specific host, ask the system administrator of the remote host to replace the software release.

If the reason is the inability to find or access a remote directory on a specific host with a specific user ID, ask the system administrator of the remote host to verify that the directory actually exists and that the specified user has read access on that directory. If the directory does not exist, the software release is missing and should be installed at the host. Otherwise, ask the system administrator of the remote host to grant the user access to the directory.

If the reason is the inability to connect to a specific host, verify that the IP address is valid and that the underlying IP network is healthy.

If the reason is the inability to find the host in the OPC host file, ask the system administrator of the OPC to add the host name in the OPC host file, or submit the software delivery specifying the remote host as an IP address instead of a host name.

If the reason is the inability to log in as a specific user on a specific host, verify that the specified user ID and password are valid on the host.

If the reason is that the OPC disk is full, get the system administrator of the OPC to delete unnecessary OPC files such as unused NE loads.

If the reason is a lack of space left on the OPC disk, get the system administrator of the OPC to delete unnecessary OPC files such as unused NE loads.

If the reason is an unsuccessful attempt to reconnect to a host after a certain number of times, verify the health of the underlying IP network.

If the reason is that the pause timer expired, there is no required action. However, you may want to resubmit the software delivery.

—end—

SDA601

Report explanation

This log report indicates a successful download of software to a network element.

Report severity

Warning

Report format

The following is the format for an SDA601 log report.

SDA601 Software download successful; load <load identifier> to <processor identifier>. <number of records> records were sent in <time> seconds.

Report example

The following is a typical example of an SDA601 log report.

```
SDA601 Software download successful; load TXP06CHIPL2 to NE 43
Sh 1. 3000 records were sent in 2 seconds.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<ne id>	Text	Location of NE processor
<load identifier>	Text	Load identifier
<number of records>	Decimal number	Number of records
<time>	Decimal number	Time to download

Action

None

—end—

SDA602

Report explanation

This log indicates that the specified network element software load was successfully transferred between the two specified OPCs. There should be a corresponding log SDA703 which indicated the beginning of this transfer.

Report severity

Warning

Report format

The following is the format for an SDA602 log report.

SDA602 Transfer success: file, <load identifier>, from <opc identifier> to <opc identifier>. The <operation type> transfer was initiated from <opc identifier>.

Report example

The following is a typical example of an SDA602 log report.

```
SDA602 Transfer success: file, TXP06CHIPL2, from opcm002 to
opcm003. The NE load transfer was initiated from opcm002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<load identifier>	Text	Load identifier
<opc identifier>	Text	OPC name
<operation type>	NE load	Network element load

Action

None

—end—

SDA605

Report explanation

This log indicates that the transfer of the specified network element software load between the two specified OPCs was cancelled by the user. There should be a corresponding log SDA703 which indicates the beginning of this transfer.

Report severity

Warning

Report format

The following is the format for an SDA605 log report.

SDA605 Transfer cancel: file, <load identifier>, from <opc identifier> to <opc identifier>. The <operation type> transfer was initiated from <opc identifier>.

Report example

The following is a typical example of an SDA605 log report.

```
SDA605 Transfer cancel: file, TXP06CHIPL2, from opcm002 to
opcm005. The NE load transfer was initiated from opcm002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<load identifier>	Text	Load identifier
<opc identifier>	Text	OPC name
<operation type>	NE load	Operation type

Action

None

—end—

SDA609

Report explanation

This log indicates that the specified network element software load was successfully transferred between the two specified OPCs. However, the current state of the receiving OPC prevents the load from being distributed to network elements. There should be a corresponding log SDA703 which indicates the beginning of this transfer.

Report severity

Warning

Report format

The following is the format for an SDA609 log report.

SDA609 Transfer success: file, <load identifier>, from <opc identifier> to <opc identifier>. The file could not be installed because <opc identifier> was inactive. The file will automatically be installed when <opc identifier> becomes active. The transfer was initiated from <opc identifier>.

Report example

The following is a typical example of an SDA609 log report.

```
SDA609 Transfer success: file, TXP06CHIPL2, from opcm002 to
opcm005. The file could not be installed because opcm005 was
inactive. The file will automatically be installed when opcm005
becomes active. The transfer was initiated from opcm002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<load identifier>	Text	Load identifier
<opc identifier>	Text	OPC name

Action

None

—end—

SDA611

Report explanation

This log report indicates that a delivery of files from the OPC to a network element has succeeded.

Report severity

Warning

Report format

The following is the format for an SDA611 log report.

```
SDA611 Install NE Delivery Files command succeeded.
```

Action

None

—end—

SDA614

Report explanation

This log report indicates that a delivery of files from the OPC to a network element has succeeded.

Report severity

Warning

Report format

The following is the format for an SDA614 log report.

SDA614 Deletion of <operation type> delivery file, <file name>, succeeded.

Report example

The following is a typical example of an SDA614 log report.

```
SDA614 Deletion of NE load delivery file, TXP06CHIPL2,
succeeded.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<operation type>	NE load	Type of operation
<file name>	Text	Name of the file

Action

None

—end—

SDA615

Report explanation

This log report indicates that a user cancelled an OPC software installation.

Report severity

Warning

Report format

The following is the format for an SDA615 log report.

SDA615 On <remote opc identifier>, user cancelled the <software release> installation.

Report example

The following is a typical example of an SDA615 log report.

```
SDA615 On opcm005, user cancelled the SX7E86AA0701
installation.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<remote opc identifier>	Text	OPC name
<software release>	Text	Name of the software release

Action

This software installation cancelling action is taken within the Remote OPC Installation tool. While still within this tool, the user can continue to cancel any other pending software installations and close the tool; or, continue with another installation; or retry a failed installation.

—end—

SDA617

Report explanation

This log report indicates that an OPC software installation completed normally. If additional software installations have been selected using the Remote OPC Installation tool, the next installation in the list is started.

Report severity

Warning

Report format

The following is the format for an SDA617 log report.

SDA617 On <remote opc identifier>, completed <software release> installation successfully.

Report example

The following is a typical example of an SDA617 log report.

```
SDA617 On opcm005, completed SX7E86AA0701 installation
successfully.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<remote opc identifier>	Text	OPC name
<software release>	Text	Name of the software release

Action

No action is required. However, you should enter the Remote OPC Installation tool to verify that all requested software installations were completed normally. If an installation failed or was aborted by a user, you should retry or cancel these installations. You may also wish to setup a new installation at this point.

—end—

SDA619

Report explanation

This log report indicates that the specified network element software load was successfully transferred between the two specified OPCs. However, the current state of the receiving OPC prevents the load from being distributed to network elements. There should be a corresponding log SDA703 which indicates the beginning of this transfer.

Report severity

Warning

Report format

The following is the format for an SDA619 log report.

SDA619 Transfer success: file, <file name>, from <opc identifier> to <opc identifier>. The <operation type> file could not be installed because <opc identifier> was not commissioned. The file will automatically be installed when <opc identifier> is commissioned. The transfer was initiated from <opc identifier>.

Report example

The following is a typical example of an SDA619 log report.

```
SDA619 Transfer success: file, TXP06CHIPL2, from opcm002 to
opcm005. The NE load file could not be installed because opcm005
was not commissioned. The file will automatically be installed
when opcm005 is commissioned. The transfer was initiated from
opcm002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<file name>	Text	Name of the file
<opc identifier>	Text	OPC name
<operation type>	NE load	Type of operation

Action

If the current state of the receiving OPC was expected to be commissioned, determine why it is not, and perform the commissioning, if appropriate.

—end—

SDA620

Report explanation

This log report indicates that an OPC data save operation has completed successfully.

Report severity

Warning

Report format

The following is the format for an SDA620 log report.

SDA620 Save OPC data to tape operation succeeded. The archive consists of <num blocks> and its checksum is <checksum>.

Report example

The following is a typical example of an SDA620 log report.

```
SDA620 Save OPC data to tape operation succeeded. The archive
consists of 47 and its checksum is 3254.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<num blocks>	Decimal number	Number of blocks of data saved
<checksum>	Decimal number	Used to validate transfer

Action

None

—end—

SDA621

Report explanation

This log report indicates that an OPC data restore operation has completed successfully.

Report severity

Warning

Report format

The following is the format for an SDA621 log report.

SDA621 Restore OPC data from tape operation succeeded. The archive consists of <num blocks> and its checksum is <checksum>.

Report example

The following is a typical example of an SDA621 log report.

```
SDA621 Restore OPC data from tape operation succeeded. The
archive consists of 47 and its checksum is 3254.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<num blocks>	Decimal number	Number of blocks of data saved
<checksum>	Decimal number	Used to validate transfer

Action

None

—end—

SDA623

Report explanation

This log report indicates that an OPC data save operation was cancelled.

Report severity

Warning

Report format

The following is the format for an SDA623 log report.

```
SDA623 Save OPC data to tape operation was cancelled by the user.
```

Action

None

—end—

SDA630

Report explanation

This log report indicates that the upgrade specified in the Network Upgrade Manager has been completed successfully. Information is provided about the software version and the nodes upgraded.

Report severity

Warning

Report format

The following is the format for an SDA630 log report.

SDA630 Upgrade completed of system software as specified by the user in the Network Upgrade Manager. Software has been upgraded to <version>. The following nodes have been upgraded: <node names>.

Report example

The following is a typical example of the SDA630 log report.

```
SDA630 Upgrade completed of system software as specified by the
user in the Network Upgrade Manager. Software has been upgraded
to OC3/OC12. The following nodes have been upgraded: backup OPC.
```

Action

None

—end—

SDA631

Report explanation

This log report indicates that the upgrade specified in the Network Upgrade Manager has been completed successfully. Information is provided about the software version and the nodes upgraded.

Report severity

Warning

Report format

The following is the format for an SDA631 log report.

SDA631 completed upgrade of software on <node name>. The OPC software load has been upgraded from <old load> and to <new load>.

Report example

The following is a typical example of the SDA631 log report.

```
SDA631 Completed upgrade of software on OPCM731B. The OPC
software load has been upgraded from opc09av_hp_80 to
opc10a0_hp_80.
```

Action

None

—end—

SDA637

Report explanation

This log report is generated the system meets the hardware baseline requirements during a software upgrade.

Report severity

Warning

Report format

The following is the format for an SDA637 log report.

SDA637 This system meets the hardware baseline requirements for <release>.

Report example

The following is a typical example of an SDA637 log report.

```
SDA637 This system meets the hardware baseline requirements for
ANrel10.00.
```

Field descriptions

The following table explains each of the variable field in the log report.

Field	Value	Description
<release>	Character string	The release name to which the system is being upgraded

Action

None

—end—

SDA638

Report explanation

This log report indicates that the network upgrade procedure has been completed successfully.

Report example

The following is an example of an SDA638 log report.

```
SDA638 The network upgrade procedure completed.
```

Action

None

—end—

SDA639

Report explanation

This log report indicates that the upgrade of the software of an OPC or NE node has been completed successfully.

Report example

The following is an example of an SDA639 log report.

```
SDA639 Upgrade step completed.
```

Action

None

—end—

SDA650

Report explanation

This log report indicates that a backup of OPC data to tape was successful.

Report severity

Warning

Report format

The following is the format for an SDA650 log report.

```
SDA650 File backup to tape was successful.
```

Action

None

—end—

SDA651

Report explanation

This log report indicates that a restoration of OPC data from tape was successful. Changes made to OPC data after the backup to this tape was performed, are lost after the restore of data from this tape. Depending on the amount of time which has passed between the data save and the restore operations, and on the type of activities which were performed in this interval, the loss of data may be significant or confusing.

Report severity

Warning

Report format

The following is format for an SDA651 log report.

```
SDA651 File restore from tape was successful.
```

Action

None

—end—

SDA652

Report explanation

This log report indicates that a network upgrade was cancelled by a user during the indicated upgrade step.

Report severity

Warning

Report format

The following is the format for an SDA652 log report.

SDA652 Network upgrade cancelled by user during <upgrade step>.

Report example

The following is a typical example of the SDA652 log report.

```
SDA652 Network upgrade cancelled by user during NE software
download.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<upgrade step>	Text string	Current operation being performed when interrupt received

Action

None

—end—

SDA653

Report explanation

This log report indicates that the indicated OPC has been successfully upgraded to the specified software release.

Report severity

Warning

Report format

The following is the format for an SDA653 log report.

SDA653 On <opc name>, completed the <new load> installation successfully. The OPC software load on <opc name> has been upgraded from <old load> to <new load>.

Report example

The following is a typical example of the SDA653 log report.

```
SDA653 On OPCM0019, completed the OPCALDMB installation
successfully. The OPC software load on OPCM00P has been upgraded
from OPC03DS to OPCALDMB.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<opc name>	String	OPC identifier
<new load>	String	The new OPC software release
<old load>	String	The previous OPC software release

Action

None

—end—

SDA654

Report explanation

This log report indicates that the OPC software release on the indicated OPC has been successfully upgraded.

Report severity

Warning

Report format

The following is the format for an SDA654 log report.

SDA654 On <opc name>, completed the <release> installation successfully.

Report example

The following is a typical example of the SDA654 log report.

```
SDA654 On OPC001P, completed the OPCALDM6 installation
successfully.
```

Field description

The following table explains the variable field in the log report.

Field	Value	Description
<opc name>	String	OPC identifier
<release>	String	Software release

Action

None

—end—

SDA655

Report explanation

This log report indicates that a network upgrade has been successfully completed for the indicated span of control. The log specifies the new software that is now running in the primary and backup OPCs, and in the network elements.

Report severity

Warning

Report format

The following is the format for an SDA655 log report.

SDA655 The span <primary> <backup> has been successfully upgraded. The OPC software load on the primary and backup has been upgraded from <old load> to <new load>. The software on each NE has been upgraded to <ne load>.

Report example

The following is a typical example of the SDA655 log report.

```
SDA655 The span OPCM001P OPCM001B has been successfully
upgraded. The OPC software load on the primary and backup has
been upgraded from OPC03DS to OPCCALDMB. The software on each
NE has been upgraded to TT48L08AF4.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<primary>	String	Name of the primary OPC in this span of control
<backup>	String	Name of the backup OPC in this span of control
<old load>	String	Previous OPC software release
<new load>	String	New OPC software release
<ne load>	String	New NE software release

Action

None

—end—

SDA656

Report explanation

This log report indicates that a NEs now have valid and current database backups on the primary (local) OPC. All NEs in this OPCs span of control have backed up their database on the primary OPC as requested by the network upgrade software.

Report severity

Warning

Report format

The following is the format for an SDA656 log report.

SDA656 Successfully forced all NE database backups. The primary OPC has received database backups for all the NEs in its span of control as requested by the network upgrade software.

Action

None

—end—

SDA701

Report explanation

This log is generated because the downloading of software to network elements may affect system performance.

Report severity

Warning

Report format

The following is the format for an SDA701 log report.

Software download in progress; load <load identifier> to <processor identifier>.

Report example

The following is a typical example of an SDA701 log report.

```
SDA701 Software download in progress; load TXP06CHIPL2 to NE 43
sh 1.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<processor identifier>	Text	Location of NE processor
<load identifier>	Text	Load identifier

Action

Postpone other system resource intensive activities until the software download is complete.

—end—

SDA703

Report explanation

This log indicates the beginning of a transfer of the specified network element software load between two OPCs.

If the transfer succeeds, an SDA602 log is generated. If the transfer succeeds, but the load cannot be installed in network elements because the receiving OPC is not commissioned, then an SDA619 log is generated.

If the transfer succeeds but the load cannot be installed in network elements because the receiving OPC is inactive, then an SDA609 log is generated.

If the transfer fails, an SDA398 log is generated.

If the transfer is cancelled by the user, an SDA605 log is generated.

Report severity

Warning

Report format

The following is the format for an SDA703 log report.

Transfer start: file, <file name>, from <opc identifier> to <opc identifier>. The <operation type> transfer was initiated from <opc identifier>.

Report example

The following is a typical example of an SDA703 log report.

```
SDA703 Transfer start: file, TXP06CHIPL2, from opcm002 to
opcm005. The NE load transfer was initiated from opcm002.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<file name>	Text	Name of the file
<opc identifier>	Text	OPC name
<operation type>	NE load	Type of operation

Action

None

—end—

SDA704

Report explanation

This log report indicates that a software installation to a remote OPC has started.

Report severity

Warning

Report format

The following is the format for an SDA704 log report.

SDA704 On <remote opc identifier>, start installing <software release>.

Report example

The following is a typical example of an SDA704 log report.

```
SDA704 On opcm005, start installing SX7E86AA0701.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<remote opc identifier>	Text	OPC name
<software release>	Text	Name of the software release

Action

None

—end—

SDA707

Report explanation

This log report indicates that a network upgrade procedure has started.

Report format

The following is the format of an SDA707 log report.

SDA707 The network upgrade procedure started. The <opcid> will be upgraded from <old release number> to <new release number>.

Action

None

—end—

SDA708

Report explanation

This log report indicates that a network upgrade has been initiated on the primary OPC.

Report severity

Warning

Report format

The following is the format for an SDA708 log report.

```
SDA Network upgrade procedure started.
```

Action

None

—end—

SDA709

Report explanation

This log report indicates that loads that existed on the backup OPC (and not the primary OPC) have been deleted. (The deletion of the listed loads was confirmed by the user of the upgrade.)

Report severity

Warning

Report format

The following is the format for an SDA709 log report.

SDA709 Extra NE loads deleted from backup OPC: <load list>.

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<load list>	Text	During an operation, if any NE loads exist on a Backup OPC but not on a Primary OPC, the user is prompted if they want to remove the obsolete load. If answered yes, then the loads are deleted and this log is generated.

Action

None

—end—

SDA712

Report explanation

This log report indicates that the installation of the OPC software release on the indicated OPC has started.

Report severity

Warning

Report format

The following is the format for an SDA712 log report.

SDA712 On <opc>, start installing <new load>. The OPC software load on <opc2> will be upgraded from <old load> to <new load>.

Report example

The following is a typical example for the SDA712 log report.

```
SDA712 On OPCM001P, start installing OPCALDMB. The OPC software
load on OPCM001P will be upgraded from OPC03DS to OPCADLMB.
```

Field descriptions

The following table explains each of the variable fields in the log report.

Field	Value	Description
<opc>	String	Name of the primary OPC on which the upgrade procedure has been installed
<new load>	String	Name of the software release to which the network is being upgraded
<opc2>	String	Name of the backup OOC, which will be upgraded first
<old load>	String	Name of the current software release in the backup OPC
<new load2>	String	Name of the new software release that will be loaded into the backup OPC

Action

None

—end—

SDA713

Report explanation

This log report indicates that the listed NE loads exist on the backup OPC and not on the primary OPC because the upgrade initiator requested that the load not be deleted.

Report severity

Warning

Report format

The following is the format for an SDA713 log report.

SDA713 Unused NE loads left on backup OPC at user’s request. The following NE loads exist on the backup OPC and not on the primary OPC: <load list>.

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<load list>	String	During an operation, if any NE loads exist on a Backup OPC but not on a Primary OPC, the user is prompted if they want to remove the obsolete load. If answered yes, then the loads are deleted and this log is generated.

Action

None

The upgrade is suspended if the NE loads remaining on the backup OPC exceed the disk space allocated for them. In this case, a log report SDA326 is generated.

—end—

SDA720

Report explanation

This log report indicates that an OPC data save operation has started.

Report severity

Warning

Report format

The following is the format for an SDA720 log report.

SDA720 Save OPC data to tape operation started.

Action

None

—end—

SDA721

Report explanation

This log report indicates that an OPC data restore operation has started.

Report severity

Warning

Report format

The following is the format for an SDA721 log report.

SDA721 Restore OPC data from tape operation started.

Action

None

—end—

SDA737

Report explanation

This log report is generated the system meets the hardware baseline requirements during a software upgrade.

Report severity

Warning

Report format

The following is the format for an SDA737 log report.

SDA737 Despite hardware baseline deficiencies, user <user name> has chosen to proceed with the software upgrade to <release>.

Report example

The following is a typical example of an SDA737 log report.

```
SDA737 Despite hardware baseline deficiencies, user root has
chosen to proceed with the software upgrade to ANrel10.00.
```

Field descriptions

The following table explains each of the variable field in the log report.

Field	Value	Description
<user name>	Character string	The id of the user issuing the upgrade
<release>	Character string	The release name to which the system is being upgraded

Action

None

—end—

SDA738

Report explanation

This log report indicates that an upgrade of the software of an OPC or NE node is starting.

Report format

The following is the format for an SDA738 log report.

SDA738 Upgrade step started.

Action

None

—end—

SOFT501

Report explanation

This log report is generated when the default mapper for STS Bandwidth Management is disabled.

Report format

The following is the format for log report SOFT501.

```
SOFT501 mmm:dd hh:mm:ss nnnn event_type event_label
     Software Functionality: <software functionality>
     Status: <status>
```

Report example

The following shows a typical example of log report SOFT501.

```
SOFT501 FEB11 16:41:51
     Software Functionality: STS Default Mapper
     Status: Disabled
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<software functionality>	STS Default Mapper	Software functionality whose status is changed
<status>	Disabled	Present state after the change

Action

None

—end—

STBY300

Report explanation

This log report indicates that the network upgrade operation has been suspended because the network upgrade manager tool has been closed.

Report severity

Warning

Report format

The following is the format for a STBY300 log report.

STBY300 The network upgrade has been suspended. Restart the Network Upgrade Mngr tool from the Session Manager to continue the network upgrade.

Action

Restarting the network upgrade manager tool may permit the upgrade process to continue. Do not take any other action. If you do, the upgrade process may be unable to continue and it will have to be restarted.

If restarting the network upgrade manager tool does not permit the upgrade to continue, it will have to be restarted.

—end—

STBY340

Report explanation

This log report indicates that an OPC could not locate its partner. This log appears under normal circumstances, during commissioning.

Report severity

Warning

Report format

The following is the format for a STBY340 log report.

STBY340 Partner OPC not found; <reason>.

Report example

The following is a typical example of a STBY340 log report.

```
STBY340 Partner OPC not found; incompatible software on OPCs.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<reason>	This OPC has not been commissioned yet: its OPC address hasn’t been assigned No partner has been commissioned for it Incompatible software on OPCs	Failure reason

Action

If the reason field indicates “This OPC has not been commissioned yet: its OPC address hasn’t been assigned”, during commissioning, replacing an OPC module, or any other process that involves changes to the OPC address, this log is normal; it is for information only. The process that puts out this log tries every two minutes to see if the address has been entered. Once the address is assigned, this log should not appear.

—continued—

STBY340, continued

If the reason field indicates “No partner has been commissioned for it”, and a network is commissioned with a primary OPC and no backup OPC, this log is normal. It is for information purposes only.

If the reason field indicates “Incompatible software on OPCs”, during the process of upgrading OPC software, this log is normal. The situation will resolve itself after the same version of OPC software has been installed on both OPCs in the network.

If no upgrade is in progress and this log appears once, it will likely correct itself and no action should be taken. However, if this log appears once per day, it may indicate a software protocol error. Typically this is because the OPCs have lost communication with one another (log STBY509 is generated). To recover from such an error, reload the OPC software onto both OPCs in the network. Use either a new tape, or the previous OPC software load that was working.

—end—

STBY356

Report explanation

During some phases of data synchronization, logs cannot be sent to the Event Browser for immediate display. Also, because data synchronization involves both OPCs in a network, the error may have occurred at either one. This log report informs you that an error did take place, and that the Event Browser must be updated.

Report severity

Warning

Report format

The following is the format for a STBY356 log report.

```
STBY356 Data sync error detected. See Event Browser on OPCs for details.
Do this by refreshing the Event Browser that is currently displayed and by
logging into the other OPC and opening the Event browser.
```

Action

The Event Browser displays only the logs affecting the OPC you are logged into. Therefore, to complete your investigation, you must log into both OPCs.

If the Event Browser is already displayed:

1. Make sure you have the correct filter set for the Events list.
2. Display the Events list menu and refresh the information in the Events list. In the active OPC, this is done by choosing the Update list command. However, this is not available in the inactive OPC. Instead, you must either close and re-open the event browser, or use the filter command. See the NTP description of the event browser for more information on the use of these commands.
3. Look for log STBY347 or STBY348.

If you are only logged into one of the OPCs involved in the synchronization:

1. Log into the other OPC now.
2. Open the Event Browser.
3. Make sure you have the correct filter set for the Events list.
4. Look for log STBY347 or STBY348.

—end—

STBY368

Report explanation

This log report is generated when one data synchronization process is running and a second request to start data synchronization is received. The second request can be either manually initiated or automatically scheduled (for example, the nightly data synchronization).

Report severity

Warning

Report format

The following is the format for a STBY368 log report.

```
STBY368 A data sync request was denied.
```

Action

If the second request is manually initiated, the user receives a response on the terminal and this log provides no additional information.

If a scheduled synchronization is denied because a user-initiated data sync between the primary and backup OPCs is running, no further action is required.

If the data sync in progress is due to recommissioning, where data between a Portable OPC and the primary OPC is being synchronized, a data sync between primary and backup OPCs is still required and should be initiated as soon as possible.

—end—

STBY372

Report explanation

This log report indicates that the regularly scheduled synchronization of data between primary and backup OPCs could not be completed, because the backup OPC is not commissioned or physically connected to the primary OPC.

Report severity

Warning

Report format

The following is the format for a STBY372 log report.

STBY372 Nightly data synchronization request ignored because backup OPC is not connected.

Action

If the system does not have a backup OPC, no action is required.

If a backup OPC has been commissioned, look for COM type logs indicating the communications error, or STBY type logs to indicate changes in the OPC state. Correct any failure condition indicated. A data synchronization can be manually initiated, if desired. See *Commissioning and Testing*, Volume 3.

—end—

STBY381

Report explanation

This log report indicates one of two possible problems.

Within one network:
If one of a Primary and Backup OPC pair has been commissioned with an incorrect address while the other received the correct addresses, the OPC with the incorrect address for its partner will issue this log. Both OPCs will attempt to take control of the network until this error is corrected.

Between two networks:
If an OPC is inadvertently given the address, not of its own partner, but of an OPC in another pair, it will send messages to that OPC. The receiving OPC will issue this log. The problem, however, resides with the other pair of OPCs, both of which vie for control of that network until the problem is solved.

Report severity

Major

Report format

The following is the format for a STBY381 log report.

STBY381 Link request rejected from OPC <opc identifier>.

Report example

The following is a typical example of a STBY381 log report.

```
STBY381 Link request rejected from OPC opcm002.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<opc identifier>	Text	OPC name

Action

If the OPC identified in the log is correct for an OPC in this network cluster, check and correct the address of that OPC in the commissioning data of the OPC which issued the log.

If the OPC identified in the log is not in the same network cluster as the OPC which issued the log, check the address of the partner OPC in the commissioning data of the specified OPC (or request the administrator of that network to perform the check).

—end—

STBY507

Report explanation

This log report is issued whenever two OPCs regain communications which were previously lost due to one of the following reasons:

- downloading of software to an NE which does not have diverse routing
- fiber cut
- failed OPC

Report severity

Warning

Report format

The following is the format for a STBY507 log report.

```
STBY507 OPC to OPC link established.
```

Action

None

—end—

STBY508

Report explanation

This log only appears during commissioning or when an OPC is re-seated in the shelf while the network is split.

Report severity

Warning

Report format

The following is the format for a STBY508 log report.

```
STBY508 OPC to OPC link not established.
```

Action

Continue with your current task. You should see an STBY507 log report when the commissioning work is completed or after the network is united.

—end—

STBY509

Report explanation

This log only appears if a network is commissioned as having a primary and a backup OPC. The log indicates a change in the standby status of the two OPCs. That is, the OPC displaying this log has lost contact with its partner.

A typical situation which would trigger this log is the downloading of software to a network element which does not have diverse routing. During this process the two OPCs in the network lose connectivity; they regain it after the download has been completed, which results in issuing the STBY507 log.

Report severity

Minor

Report format

The following is the format for a STBY509 log report.

STBY509 OPC to OPC link lost.

Action

If a task is being performed which legitimately causes a loss of communication between the OPCs, continue the task and ensure that an STBY507 log report is generated when the task has been completed.

If the loss of communication is unexpected, log in to the OPC which did not generate the log report and check its status. If it is functioning normally, look for a problem in the communication link between the OPCs.

—end—

STBY510

Report explanation

This log report indicates a change in status of the OPC which generated the log.

Report severity

Warning

Report format

The following is the format for a STBY510 log report.

STBY510 OPC has become <activity identifier>.

Report example

The following is a typical example of a STBY510 log report.

```
STBY510 OPC has become Active.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<activity identifier>	Active Inactive	Status of the OPC

Action

None

—end—

STBY600

Report explanation

This log is generated at the backup OPC to indicate that the network upgrade has been completed.

Report severity

Warning

Report format

The following is the format for a STBY600 log report.

STBY600 The network upgrade has been completed. This backup OPC has resumed normal operations. A STBY510 log is generated if the status of this OPC has changed.

Action

If the STBY510 log appears, the backup OPC will have returned to the inactive state. Surveillance can no longer be performed from the backup OPC. Surveillance administrators should log out of the backup OPC and log in to the primary OPC.

—end—

STBY601

Report explanation

This log is generated at the primary OPC to indicate that the network upgrade has been completed.

Report severity

Warning

Report format

The following is the format for a STBY601 log report.

STBY601 The network upgrade has been completed. This OPC will regain control of the network. The backup OPC should become inactive.

Action

None

—end—

STBY602

Report explanation

This log is generated to indicate that the network upgrade has been completed.

Report severity

Warning

Report format

The following is the format for a STBY602 log report.

STBY602 The network upgrade has been completed. This OPC will regain control of the network.

Action

None

—end—

STBY612

Report explanation

This log report indicates a successfully completed data synchronization between OPCs.

Report severity

Warning

Report format

The following is the format for a STBY612 log report.

```
STBY612 OPC data sync successful.
```

Action

None

—end—

STBY700

Report explanation

This log is generated at the backup OPC to indicate that the network is being upgraded. It warns that network surveillance will be split and that surveillance of an increasing part of the network must be performed at the backup OPC, which will become active.

Report severity

Warning

Report format

The following is the format for a STBY700 log report.

STBY700 A network upgrade has been initiated. This backup OPC is now active and available to control network elements as they are upgraded.

Action

Surveillance personnel must log in to the active backup OPC, in order to maintain surveillance over the network. Initially, no network elements will have associations with the backup OPC (that is, the surveillance tool will show the question mark symbol (?) beside the list of network elements). However, as the upgrade proceeds, all network elements will gradually come under the control of the backup OPC.

—end—

STBY701

Report explanation

This log is generated at the primary OPC to indicate that the network is being upgraded. It warns that network surveillance will be split and that surveillance of an increasing part of the network must be performed at the backup OPC, which will become active.

Report severity

Warning

Report format

The following is the format for a STBY701 log report.

STBY701 A network upgrade has been initiated. This backup OPC will become active to control network elements as they are upgraded.

Action

Surveillance personnel must log in to the active backup OPC, in order to maintain surveillance over the network. Initially, all network elements will have associations with the primary OPC (that is, the surveillance tool will show no question mark symbol (?) beside the list of network elements). However, as the upgrade proceeds, all network elements will gradually come under the control of the backup OPC, and the “?” symbol will appear beside these network elements in the surveillance tools lists, at the primary OPC.

—end—

STBY702

Report explanation

This log is generated because the synchronization of data may affect system performance.

Report severity

Warning

Report format

The following is the format for a STBY702 log report.

```
STBY702 OPC data sync is in progress.
```

Action

It may be desirable to postpone other system resource intensive activities until the data synchronization is complete.

—end—

STBY703

Report explanation

This log is generated at the primary OPC to indicate that the network upgrade is in its final stages. The last element to be upgraded is the primary OPC, which must be removed from service during this process.

Report severity

Warning

Report format

The following is the format for a STBY703 log report.

```
STBY703 Network element upgrade has been completed. While this OPC is
being upgraded, it will be out of service. During this period, the backup OPC
will control the network elements.
```

Action

Log out of the primary OPC and wait about 15 minutes for the login prompt, which indicates that the upgrade of the primary is completed. Network surveillance can be maintained from the backup OPC during this period.

—end—

STBY704

Report explanation

This log is generated at the primary OPC to indicate that a specific network element has been placed under the control of the backup OPC. An instance of this log report should be seen for all network elements in the network.

Report severity

Warning

Report format

The following is the format for a STBY704 log report.

STBY704 Network element <equipment identifier> has been placed under the control of the backup OPC, during network upgrade. A corresponding STBY500 log will appear at the backup OPC.

Report example

The following is an example of a STBY704 log report.

```
STBY704 Network element 43 has been placed under the control of
the backup OPC, during network upgrade. A corresponding STBY500
log will appear at the backup OPC.
```

Field descriptions

The following table explains the variable field in the log report.

Field	Value	Description
<equipment identifier>	Decimal number	Network element number

Action

Step	Action
1	At the end of an upgrade, ensure that a log of this type has been produced for all network elements involved in the upgrade.
2	Is a log missing?

If	Then
yes	go to step 3
no	you are finished with this procedure

—continued—

STBY704, continued

Step	**Action**
3	Use the lomui command to verify that the NE for which the log is missing is running the correct load. At the OPC prompt, type: **lomui query_loads** *A list of all the loads installed on the NE appears.*
4	Does the correct software load exist?

If the correct software load	**Then**
exists	you are finished with this procedure
does not exist	contact your next level of support

—end—

STBY705

Report explanation

This log indicates that restarting the network element upgrade manager tool has successfully resumed the network upgrade process. It is produced to acknowledge that the corrective action suggested by the STBY300 log has been effective. If this log does not appear in this situation, the network upgrade must be restarted from the beginning.

Report severity

Warning

Report format

The following is the format for a STBY705 log report.

```
STBY705 The network upgrade has resumed.
```

Action

None

—end—

STBY707

Report explanation

This log indicates that the upgrade of the network element has started.

Report severity

Warning

Report format

The following is the format for a STBY707 log report.

STBY707 Starting upgrade of network elements. The primary OPC remains active to control network elements, as they are upgraded.

Action

None

—end—

SWCT101

Report explanation

This log is generated when a switch of activity (SWACT) of the processor card on a network element has occurred. A log is generated for both the active and inactive processors.

Report format

The following is the format for a SWCT101 log report.

```
SWCT101 mmm:dd hh:mm:ss nnnn INFO SWACT
   <SWACT type> SWACT occurred at <mm>-<dd>-<hh>:<mm>:<ss>
   NE: <NE id and name>                EQP:<processor card type>
   Newly active processor: <processor>
   Newly inactive processor: <processor>
   Source: <source>
   <fault status>
           [List of active faults]
```

Report example

The following is a typical example of a SWCT101 log report.

```
SWCT101 DEC05 17:49:42 0100 INFO SWACT
   CP SWACT occurred at Dec-05 17:49:42
   NE: 27                      EQP:ABM RFT
   Newly active processor: A
   Newly inactive processor: B
   Source: System
   Active Faults:
         121 124 125 145
```

—continued—

SWCT101, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<SWACT type>	CP COLD	SWACT type
<NE id and name>	string	ID and name of the network element on which the SWACT occurred
<processor card type>	ABM FCOT ABM RFT TBM FCOT	Shelf on which the SWACT occurred
<processor>	A or B	Processor unit A or B
<source>	System User Recovery Unknown	Source that caused the SWACT to occur
<fault status>	Active faults No fault information available	If communication between the processors is available, this field displays “Active faults” and lists the faults on the following line. If the processor are not able to communicate for any period of time, this field displays “No fault information available”.

Action

None

—end—

TAC300

Report explanation

This log is generated as a result of a maintenance event, or a failure detected by the test access card (TAC) software.

> ***Note:*** Communication faults are a result of a number of errors within a specific time interval. For example, if 5 interrupt lost errors occur within 5 minutes, then a fault report is generated.

Report format

The following is the format for log report TAC300.

```
TAC300 mmm:dd hh:mm:ss nnnn event_type event_label
     Resource: <class>   Event: <event>
```

Report example

The following are typical examples of log report TAC300.

```
TAC300 MAY12 12:34:56 1234 TBL TAC Fault
     Resource: Metallic   Event:DELAY FAIL

TAC300 MAY12 12:34:56 1234 TBL TAC Fault
     Resource:Digital     Event:MOH1B FAIL
```

Field descriptions

The following table explains each of the fields in this log report.

—continued—

TAC300, continued

Field	Value	Description
<class>	Text string:	TAC maintenance identifier
	Metallic Digital IDL Communication	
<event>	Text string:	Describes the TAC event:
	Relay Fault Power loss Shelf test bus fault No talk battery ret	Metallic events
	DTAC Fail DSPI Fail MOH1A Fail MOH1B Fail Phase Lock Loop A Phase Lock Loop B	Digital events
	IDL1 Loss Phase IDL1 Loss Clock IDL1 Loss Sync IDL2 Loss Phase IDL2 Loss Clock IDL2 Loss Sync	IDL events
	Message corrupt SMI Error Buffer Full Interrupt Lost Spurious Interrupt Parity Error	Communication events
	Software Fault CODEC	System fault events

Action

If a metallic fault is reported, place the TAC out of service, then return it to service. Diagnostics are run automatically when returning the TAC to in service. If the TAC continues to fail, replace the TAC as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

—continued—

TAC300, continued

If a digital fault is reported, the TAC attempts to repair the fault on its own. If a digital fault report is not followed by a digital fault clear report, first investigate and clear any AIC faults which may have affected the TAC digital side. If the problem persists, place the TAC out of service, then return it to service. Diagnostics are run automatically when returning the TAC to in-service. If the TAC continues to fail, replace the TAC as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

If an IDL fault is reported, place the TAC out of service, then return it to service. Diagnostics are run automatically when returning the TAC to in-service. If the TAC continues to fail, replace the TAC as outlined in *Module Replacement Procedures,* 323-3001-547 in *Maintenance,* Volume 5C.

The processor will reset the TAC when it receives a communication fault, which should clear the problem. If the problem consistently reappears, contact Norther Telecom customer support and report the problem.

If a system fault is reported, the system attempts to repair the fault on its own. If the system fails to repair the fault, the TAC equipment alarm “Circuit pack fail” is raised. Look up the alarm in *Alarm and Trouble Clearing Procedures*, 323-3001-543 in *Maintenance,* Volume 5A, and proceed accordingly. If a TAC equipment alarm is not raised, the TAC is recovering automatically and no action is required.

—end—

TAC301

Report explanation

This log is generated when a test access card (TAC) restart fails.

Typically, if there is a TAC restart problem, this log follows a TAC720 log report.

Report format

The following is the format for log report TAC301.

```
TAC301 mmm:dd hh:mm:ss nnnn event_type event_label
     Reason:<reason>    Problem id:         <id number>
```

Report example

The following is a typical example of log report TAC301.

```
TAC301 MAY12 12:34:56 1234 TBL TAC Restart Fail
     Reason:Pre-kernel Diag Fail     Problem id:407
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<reason>	Text string: Restart Fail HW Init Fail Pre-kernel Diag Fail Card not a TAC Loader Fail OPC Comm Fail Load Corrupt Init Msg Timeout Abort	Reason for restart failure
<id number>	Integer	An ID given to the problem

Action

If the reason is one of Restart Fail, HW Init Fail, Loader Fail, Init Msg Timeout, or Abort, try to reload the TAC. If the TAC fails again, try removing and reinserting the TAC. If this also fails, replace the TAC, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

—continued—

TAC301, continued

If the fail reason is Pre-Kernel Diag Fail, replace the TAC, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

If the fail reason is OPC Comm. Fail, there is a problem with the link between the OPC and the processor. Try downloading the TAC again, and if the TAC fails, check the links.

If the fail reason is Load Corrupt, try downloading the TAC again. If the failure persists, contact Nortel Networks field support.

—end—

TAC500

Report explanation

This log indicates that a card was removed from one of the slots associated with the TAC circuit pack group.

Report format

The following is the format for log report TAC500.

```
TAC500 mmm:dd hh:mm:ss nnnn event_type event_label
     NE:              <NE id> < NE name>
     Shelf:           CE
     Slot:            <slot number>
     Card type:       <card type>
```

Report example

The following shows typical examples of log report TAC500.

```
TAC500 MAY12 12:34:56 1234 INFO Card Removal
     NE:              12 FCOT1
     Shelf:           CE
     Slot:            51
     Card type:       TBP
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<slot number>	20, 51, 52, or 53	Slot from which the card was removed
<card type>	TAC, TAP, TBP, or PGTC	Type of card removed from the slot

Action

Insert the correct card in the slot indicated by this log, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

—end—

TAC501

Report explanation

This log indicates that a card was inserted into one of the slots associated with the TAC circuit pack group.

Report format

The following is the format for log report TAC501.

```
TAC501 mmm:dd hh:mm:ss nnnn event_type event_label
     NE:                <NE id> < NE name>
     Shelf:             CE
     Slot:              <slot number>
     Card expected:     <card type expected>
     Card inserted:     <card type inserted>
     PEC:               <PEC>
     lot state:         <state>
```

Report example

The following shows typical examples of log report TAC501.

```
TAC501 MAY12 12:34:56 1234 INFO Card Insertion
     NE:             12 FCOT1
     Shelf:          CE
     Slot:           20
     Card expected:  TAC
     Card inserted:  Unknown
     PEC:            NT4K55AA
     Slot state:     Mismatched
```

—continued—

TAC501, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<slot number>	20, 51, 52, or 53	Slot into which the card was inserted
<card type expected>	TAC, TAP, TBP, or PGTC	Type of card expected to be inserted into the slot
<card type inserted>	TAC, TAP, TBP, PGTC, or unknown	Type of card actually inserted into the slot.
<PEC>	alphanumeric string, or Unknown	Product equipment code of the card inserted into the slot. If the PEC is from a card that is not part of the TAC circuit pack group, "Unknown" appears.
<state>	Equipped, or Mismatched	The state of the card inserted. Equipped indicates that the correct card was inserted. Mismatched indicates that an incorrect card was inserted.

Action

If the slot state is Equipped, no action is required.

If the slot state is Mismatched, and the inserted card can be identified, by the card type or PEC, remove the mismatched card and insert the correct card, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

If the slot state is Mismatched, and the inserted card is unknown, replace the card, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance,* Volume 5C.

—end—

TAC600

Report explanation

This log is generated when the TAC restart completes successfully. This log should be generated after every TAC720 restart log, if the restart is successful.

Report format

The following is the format for log report TAC600.

```
TAC600 mmm:dd hh:mm:ss nnnn event_type event_label
     Restart complete
```

Report example

The following shows typical examples of log report TAC600.

```
TAC600 MAY12 12:34:56 1234 INFO TAC Restart Pass
     Restart complete
```

Action

None

—end—

TAC700

Report explanation

This log indicates that a previously reported digital fault has been cleared.

Report format

The following is the format for log report TAC700.

```
TAC700 mmm:dd hh:mm:ss nnnn event_type event_label
     Resource: <type>    Event: FAULT CLEAR
```

Report example

The following shows typical examples of log report TAC700.

```
TAC700 MAY12 12:34:56 1234 INFO TAC Digital
     Resource: Digital    Event: FAULT CLEAR
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<type>	Digital	Indicates the type of TAC resource for which the fault was cleared.

Action

None

—end—

TAC720

Report explanation

This log is generated when a TAC undergoes a reset.

A “Reboot in progress” involves initializing TAC hardware, downloading TAC software from the OPC, and causing full TAC on-board software initialization. A “Cold reset in progress” causes full on-board TAC software initialization with no software download. A “Warm reset in progress” performs a reset of the TAC metallic side relays with no on-board software initialization.

Report format

The following is the format for log report TAC720.

TAC720 mmm:dd hh:mm:ss nnnn event_type event_label
    <text>

Report example

The following shows typical examples of log report TAC720.

```
TAC720 MAY12 12:34:56 1234 INFO TAC Restart
     Reboot in progress
```

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<text>	One of the following text strings appears: Reboot in progress Cold reset in progress Warm reset in progress	Indicates the type of TAC reset in progress.

Action

None

—end—

TAC900

Report explanation

This log is generated when a TAC sanity timeout occurs, when pSOS detects a fatal error, or when an TAC task traps.

Report format

The following is the format for log report TAC900.

TAC900 mmm:dd hh:mm:ss nnnn event_label
    <errno> <type> <vector> <taskname>
    <statusreg>
    <illaddr>
    <traceback>

Report example

The following are typical examples of log report TAC900.

```
TAC900 MAY01 11:51:38 4100 TBL TAC Task TRAP
     UNEXPECTED EXCEPTION

TAC900 MAY01 11:51:38 4200 TBL TAC Task TRAP
     SANITY TIMEOUT vector = 1f

TAC900 MAY01 11:51:38 4300 TBL TAC Task TRAP
     errno = 1961 FATAL ERROR
     006108b4
     0063d1e4
     deaddead

TAC900 MAY01 11:51:38 4300 TBL TAC Task TRAP
     BUS ERROR vector = 2 task name = 00170000
     sr = 3000
     ill addr =0
     006108b4
     0063d1e4
     deaddead
```

—continued—

TAC900, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<errno>	int32 in decimal	The error number. This field exists only if <type> is FATAL ERROR or EXIT. If<type> is FATAL ERROR, errno is the return code from pSOS. If<type> is EXIT, errno is the return code from the task.
<type>		The error type can take the following values:
	UNEXPECTED EXCEPTION	— unexpected exception
	SANITY TIMEOUT	— sanity timeout
	FATAL ERROR	— pSOS fatal error
	EXIT	— task exit
	PARITY ERROR	— parity error while the TAC is master of the bus
	BUS ERROR	— bus error task trap
	ADDRESS ERROR	— address error task trap
	ILLEGAL INSTRUCTION	— illegal instruction task trap
	DIVIDE BY ZERO	— divide by zero task trap
	PRIVILEGE VIOLATION	— privilege violation task trap
<vector>	int32 in decimal	The vector number corresponding to the task trap. Present only if <type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.
<taskname>	int32 in hex, or 4 alphanumeric characters	The name or id of the task that trapped. Present only if <type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.
	—continued—	

—continued—

TAC900, continued

Field	Value	Description
<statusreg>	int16 in hex	The contents of the CPU status register when the trap has occurred. Present only if <type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.
<illaddr>	int32 in hex	The illegal address that caused the bus or address task trap. Present only if <type> is BUS ERROR or ADDRESS ERROR.
<traceback>	set of int32 in hex, normally terminated by "deaddead".	Set of addresses showing the nesting of functions when the software error occurred. Present only if <type> is PARITY ERROR, BUS ERROR, ADDRESS ERROR, ILLEGAL INSTRUCTION, DIVIDE BY ZERO, or PRIVILEGE VIOLATION.
—end—		

Action

This log should be forwarded to Nortel Networks customer support for problem diagnosis and corrective action.

—end—

TAC901

Report explanation

This log is generated by TAC applications whenever a software error is detected. A software error is an unexpected software condition, such as out of bound input arguments passed to a function.

Report format

The following is the format for log report TAC901.

```
TAC901 mmm:dd hh:mm:ss  event_label
     <sectionName> <lineNumber>
     <traceback>
     (|string|) <int32>
```

Report example

The following shows a typical example of log report TAC901.

```
** TAC901 MAY12 12:34:56 TBL TAC SOFTWARE ERROR
     hmfmi2.ab01 1961
     0061dece
     0061b230
     006638b8
     0061ad5e
     0061b0bc
     deaddead
     1

** TAC901 MAY12 12:34:56 TBL TAC SOFTWARE ERROR
     hmfmi2.ab01 1961
     0061dece
     0061b230
     006638b8
     0061ad5e
     0061b0bc
     deaddead
     Cannot allocate memory 2
```

—continued—

TAC901, continued

Field descriptions

The following table explains each of the fields in this log report.

Field	Value	Description
<sectionName>	Alphanumeric	Section name
<lineNumber>	Numeric	Line number
<traceback>	Set of int32 in hex, normally terminated by “deaddead”	Set of addresses showing the nesting of functions when the software error occurred.
<string>	String of characters	Optional field. String of characters provided by the application which generates the SWERR, to give some indication about the software error.
<int32>	int32 in decimal	Application generated long word data to give some information about the software error, typically a bad return code.

Action

This log should be forwarded to Nortel Networks customer support for problem diagnosis and corrective action.

—end—

TPS100

Report explanation

This log report is generated when there is a failure anywhere in the system. It can also be generated when normal maintenance or diagnostics are being performed. This log is for informational use only.

Report format

The following is the format for log report EQP326.

```
TPS100 mmm:dd hh:mm:ss ssdd FLT TPS IH ERROR
TRBLINFO=trbtxt   PRIO=nnnn   SUBC=nnnn
SRC_MTA=hhhh hhhh hhhh hhhh DST_MTA=hhhh hhhh hhhh hhhh
INTERNAL_MTA_NAME=name
PROTOCAL=name
SIGNAL=NN
UID=hhhh hhhh
MSG_HDR=hhhh hhhh hhhh
MSG=hhhh hhhh hhhh
```

Report example

The following shows a typical example of log report TPS100.

```
CM            TPS100 FEB19 15:30:32 8900   FLT  TPS
IH ERROR
TRBLINFO = SCBLETTER_OVFLW  PRIO= 0003  SUBC=0001
SRC_MTA = FFFF FFFF FFFF FFFF   DST_MTA = 4000 FFFF
C329 0000
INTERNAL_MTA_NAME =  NIL
PROTOCOL   =
SIGNAL     = 1
UID        = 00B3 14E1
MSG_HDR    = FF32 C001 FF00
MSG = 0142 FFFF FFFF
```

In this example SCBLETTER_OVFLW is the 'type' of TPS100 log.

—continued—

TPS100, continued

Field descriptions

The following table explains the possible fields in the log report.

Field	Value	Description
FLT TPS IH ERROR	Constant	Indicates the TPS input handler encountered an error in a received message.
TRBLINFO	NIL_TROUBLE_CODE	Indicates the trouble code for reasons that are not covered by the rest of the trouble codes used by the handler when it gets a message from the MTS that is not bound for a TPS destination.
	NO_SCBS	Indicates no subnet control block (SCB) left in the system to allocate to a new instance upon arrival of a message
	INVALID_LNAME	Indicates the local name of the destination TPS application is incorrect.
	BAD_MTA_OFFSET	Indicates no instance at the offset in the message.
	INVALID_UID	Indicates the user identifier (UID) is invalid.
	SCBLETTER_OVERFLOW	Indicates too many SCB letters enqueued to the SCB.
	BMS_Q_PRB	Indicates the buffer containing the message could not be enqueued on its destination SCB due to corruptions in that queue.
	NO_MASTER_BOUND	Indicates a message was sent to a TPS master that has not been bound in, causing the TPS input handler to fail to find the destination TPS application.
	MTS_OUT_FAILURE	Indicates a message transmission from the TPS to the MTS layer failed.
	MESSAGE_USAGE_EXCEEDED	Indicates a TPS application attempted to use more resources than it was allocated.
	NIL_SCBLONGQ	Indicates the TPS input handler received a long message (greater than 128 bytes of application data) with no long message buffers allocated in the system.

—continued—

—continued—

TPS100, continued

Field	Value	Description
	NO_LONG_BUF_AVAIL	Indicates the TPS input handler received a long message (greater than 128 bytes of application data) with no long message buffers allocated for the application.
	MP_ERROR	Indicates the message prescreener for the application found a problem with the received message and discarded it.
PRIO	0000-FFF	Indicates the SOS class.
SUBC	0000-FFF	Gives extra information for NT debugging purposed.
SRC_MTA	0000-FFF	Indicates the source of the message.
DST_MTA	0000-FFF	Indicates the destination of the message.
INTERNAL_MTA_ NAME	Character string	Indicates the node portion of the MTA.
PROTOCOL	Character string	Indicates the protocol of the message.
SIGNAL	0 - 32767	Indicates the signal of the message.
UID	0000-FFF	Indicates the user identifier.
MSG_HDR	0000-FFF	Indicates internal routing information.
MSG	0000-FFF	Gives the first 3 words of the message.

—end—

Action

None.

—end—

VLCM406

Report explanation

This log report indicates that the DMS-10NA switch’s line provisioning has failed. The DMS-10NA requested that the AccessNode provision, deprovision, reprovision, or change the line state of a line and the AccessNode failed to implement the switch’s provisioning request.

In a multi-hosting environment, the switch’s provisioning request may have failed because the line was already provisioned by another switch.

Report format

The following is the format for log report VLCM406:

```
      VLCM406 mmmdd hh:mm:ss nnnn INFO Prov/Deprov
Log Text:  VLCM Switch Provisioning/Deprovisioning Action
Result:    <result>
NE:        <NE>
Location:  <frame>
VLCM:      <VLCM#>
LSG:       <drawer>
Line:      <line card>
```

Report example

The following shows a typical example of log report VLCM406:

```
      VLCM406 Dec09 20:05:03 0802 INFO Prov/Deprov
Log Text: VLCM Switch Provisioning/Deprovisioning Action
Result:    Line provisioning failed
NE:        11 Hoover
Location:  1
VLCM:      1
LSG:       0
Line:      25
```

—continued—

VLCM406, continued

Field descriptions

Table 5-2 explains each of the variable fields in this log report.

Table 5-2
VLCM406 field descriptions

Field	Value	Description
<result>	One of the following text strings:	Result of the switch's provisioning request:
	Line state change failed	The state of the line card has not been changed.
	Line provisioning failed	The line has not been provisioned.
	Line deprovisioning failed	The line has not been removed.
	Line reprovisioning failed	The line has not been reprovisioned to another service.
<NE>	Integer and text string	The indicated network element's number and name.
<frame>	Integer	Frame identifier
<VLCM#>	Integer	The virtual line concentration module (VLCM) number of the line.
<drawer>	0 to 19	The VLCM drawer number of the line.
<line card>	0 to 31	The VLCM line card number of the line.

Action

Step	Action
1	Perform the provisioning, deprovisioning, reprovisioning, or line state action again.

If the action	Then
succeeds	End the procedure.
does not succeed	Go to step 2.

—continued—

VLCM406, continued

Step	Action
2	From the network element user interface (NE UI), post the line by entering:

eq lcmlc <vlcm> <lsg> <slot> ↵

where

<vlcm>	the vlcm number: **1** to **2**
<lsg>	the line card drawer number: **0** to **19**
<slot>	the line card number: **0** to **31**

The LC Equip screen appears.

3 Determine if another switch has provisioned the line.

If another switch	Then
has provisioned the line	Delete the line off of the DMS-10NA switch and end the procedure.
has not provisioned the line	Go to step 4.

4 Delete the line and re-add it at the DMS-10NA switch.

5 Perform the provisioning, deprovisioning, reprovisioning, or line state change action.

If the action is	Then
successful	End the procedure.
not successful	Contact your next level of Nortel Networks support.

—end—

Appendix A: Standard log data

This chapter describes log report fields which are standard for most logs.

Header information

Each log report has a header which contains several fields of information. Each field is explained below.

alarm log_name log_# mmm:dd hh:mm:ss nnnn event_type event_label

alarm: the alarm indicator shows the severity (if any) of a log
  *** critical alarm
  ** major alarm
  * minor alarm
  absence of an asterisk indicates no alarm condition

log_name: two to four characters identifying the name of the log

log_#: always three digits identifying the log number

mmm: three-character abbreviation for the month (JAN to DEC)

dd: two-digit number representing the day of the month (01 to 31)

hh: two-digit number representing the hour of the day (00 to 23)

mm: two-digit number representing the minute of the hour (00 to 59)

ss: two-digit number representing the seconds of the minute (00 to 59)

nnnn: four-digit number, the first two of which represent the global sequence number of the log (00 to 99), and the last two of which represent the device sequence number of the log (00 to 99) event_type: four characters representing one of several log event types:

blank
FLT
INFO
FAIL
PASS
SUMM
TBL

event_label: variable length field which summarizes the log report

Log location fields

The location information contained in many log reports varies according to the object that generated the log report. The following examples illustrate the possible log location information formats for different object classes. See “Explanation of variable location fields” on the next page for an explanation of each variable shown in the following examples.

Equipment

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1              LOCATION: n2 s2
     EQP: n3 s3
```

Frame

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1              LOCATION: n2 s2
```

Shelf

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1              LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4          SHELF: s8
```

Circuit pack

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1              LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4          SHELF: s8
     SLOT: n6               SUBSLOT: n7
     SERVICE CLASS: c1
     CIRCUIT PACK HW: h1
```

Circuit pack group

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1                LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4            SHELF: s8
     CPG: s4 s5               SLOT: n8 n9 n10   SUBSLOT: n11
```

ESI circuit pack group

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1                LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4            SHELF: s8
     CPG: s4 s5               SLOT: n8          SUBSLOT: n11
```

Redundancy (protection) group

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1                LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4 n11 n12    SHELF: s8 s9 s10
     PROTECTN GRP: n16        TYPE: s6
```

Redundancy (protection) group member

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1                LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4 n11 n12    SHELF: s8 s9 s10
     PROTECTN GRP: n16        MEMBER: s6 s7
```

Explanation of variable location fields

Each of the variable location fields found in a log report are explained below.

n1 - network element number

n2 - frame ID

n3 - equipment (node) ID

n4, n11, n12 - position of shelves in a frame

n6 - slot or circuit pack ID

n7 - subslot or sub circuit pack ID

n8, n9, n10 - slots occupied by circuit pack group

n11 - subslot occupied by circuit pack group or ESI n16 - protection group ID

s1 - network element name

s2 - frame location name

s3 - node function (access)

s4, s6 - circuit pack group type (ESI, MIC, OC12, DS1, OPC, Proc, TIC, AIC, or TAC)

s5, s7 - circuit pack group name (a, b g1, g2, etc.)

s8, s9, s10 - unique shelf identifiers (CE, CDS 1 to CDS 7, or ANX 1 to ANX 28)

c1 - service class of a line card: FXO, FXS, DPT, DPO, TOO, TOS, ETOO, ETOS, UVG, POTS, COIN LGB, LSR, EBS, DDS, DX, TO, ETO, EM, TDM, PLR, or ISDN_U

h1 - type of line card hardware: O2WS LC (Omega 2-wire station line card), O2WO LC (Omega 2-wire Office line card), O4W LC (Omega 4-wire line card), or O68W LC (Omega 68W LC)

GR-303 logs

No new logs have been identified for this feature. However, existing log messages that report line card service type have been modified to report the new GR-303 MVI line card services. The affected field is SERVICE CLASS, as explained in the “Circuit pack” topic.

Circuit pack

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1                LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4            SHELF: s8
     SLOT: n6                 SUBSLOT: n7
     SERVICE CLASS: c1
     CIRCUIT PACK HW: h1
```

c1 - values for service class of a line card: FXO, FXS, DPT, DPO, TOO, TOS, ETOO, ETOS, UVG, POTS, COIN, LGB, LSR, EBS, DDS, DX, TO, ETO, EM, TDM, PLR, ISDN_U, MVIPOTS, MVICOIN, MVIUVG, MVILRB, or GR303_ISDN

AccessNode Express line card logs

No new logs have been identified for AccessNode Express (ANX) line cards. However, existing log messages that report line card shelf positions have been modified to report the new ANX line card positions. The affected field is SHELF, as explained in the “Circuit pack” topic.

Circuit pack

```
EQP123 MAY12 12:34:56 4321 INFO Log location field formats
     NE: n1 s1               LOCATION: n2 s2
     EQP: n3 s3
     SHELF POS: n4           SHELF: s8
     SLOT: n6                SUBSLOT: n7
     SERVICE CLASS: c1
     CIRCUIT PACK HW: h1
```

Index

SONET Products

AccessNode

Log Report Manual

The information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

Publication number: 323-3001-840
Document release: Issue 3.0
Date: October 1999
Printed in Canada