Carrier VoIP

USP Fault Management

NN10071-911

Document status: Standard
Document version: 08.02
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

New in this release

The following sections detail what's new in *USP Fault Management* (NN10071-911) for release (I)SN09U.

Features

No feature changes affect this document in this release.

Other changes

See the following section for information about changes that are not feature-related:

Changes to procedure, Replacing mission cards or TMs in system nodes

To improve usability, clarifications were made to procedure "Replacing mission cards or TMs in system nodes" (page 176).

USP Fault Management

The Universal Signaling Point (USP) displays alarms on a window of the USP GUI. Users can receive notification of the following types of faults:

- alarms
- communications application module (CAM) shelf indicators
- OAMP workstation and networking errors

The sections in this guide describe how to select, view, print, and clear faults, and their related logs, if applicable.

View System Node Alarms

Viewing system node alarms

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical View**.
3	Right-click on the desired system node. Click the **View alarms** option from the drop-down menu.
	—End—

View Alarms

Viewing alarms

Step	Action
	At the OAMP workstation
1	Click **Fault >alarm**.
2	Click the **Realtime** tab. You can change the order of the alarms by right-clicking on any column heading. When you right-click on a column heading, a drop-down menu appears with sort column ascending and sort column descending options. You can also change the order of the alarms by left-clicking on a column heading. There are 11 data fields for each alarm. The following table lists and describes the fields displayed in the **Realtime** Data window.
	—End—

Alarm descriptions

Alarm descriptions

Field Name	Description
log severity	Alarm severity of MINOR, MAJOR, or CRITICAL.
log-description	Details of the event that generated the alarm.
log-date-time	Date and time the alarm was recorded.
alarm-status	OPEN for open alarms or Acknowledged for acknowledged alarms. Once the system clears an alarm, it no longer appears on the Alarms window, but it still appears in the Logs window.
log-group-name	The subsystem that generated and identified the alarm.
log-number	The number the system assigns to each alarm. When it is paired with the group information, the number uniquely identifies each alarm.
shelf	Provides the shelf location of the equipment generating the alarm.
slot	Provides the slot location of the equipment generating the alarm.
system-node-name	The system node that generated the alarm.

An alarm banner also provides the total of each type of alarm (critical, major, and minor). It is located in the bottom panel on the left side of the main window. Double-click on any of the three color-coded areas in the alarm banner to display all current alarms and related fields in a **Realtime** Data window.

If a color-coded area in the alarm banner is flashing, there are unacknowledged critical alarms. To acknowledge an alarm means to turn if off. The intention of the flashing element is to indicate that there are new critical alarms in the system.

Adding and removing fields from Real-time data display

Step	Action
	At the OAMP workstation
1	Click **Fault >alarm**.
2	Click **Realtime**.
3	Place the cursor over any of the column headings or column cells with information about the alarms, and then right-click on the selected area.
4	Select the **customize** option from the drop-down menu that appears. Then a **Columns** panel will appear.
5	You can choose to display or remove a field from display by left-clicking on the box beside a field. A check beside a field name allows you to display a field. If you left-click on a check to remove it, then you are removing the field from display in the **Realtime** Data window. You may remove more than one item. The default shows all alarm fields. When you highlight or select a field name from Columns panel list, you can move the location of a field in the **Realtime** Data window. You can move a field toward the front or back of the column headings by left-clicking on the field name and the Move Up or Move Down button. Your changes automatically appear in the **Realtime** Data window. They remain after you exit a session.
	—End—

Select Alarms

The system allows you to acknowledge individual alarms. If you have visible or audible alarm indicators, acknowledging an alarm turns them off.

ATTENTION
When you acknowledge an alarm on the USP or USP Compact, it does not clear the indicators.

Acknowledging an alarm does not affect the status of the problem that caused the alarm. The system clears each alarm internally when the problem is resolved. To solve the specific alarm, refer to the fault-clearing procedure for that alarm.

Acknowledging alarms

Step	Action
	At the OAMP workstation
1	Click **Fault >alarm**.
2	Click the alarm you want to acknowledge.
3	Right-click the selected alarm and choose **add to posted set** from the drop-down menu. An "x" will appear beside the row.
4	Click **Acknowledge**. A confirmation dialog box appears.
5	Click **Yes**.

—End—

Export Logs and Alarms

Exporting alarms

Step	Action
	At the OAMP workstation
1	Click **Fault>alarm**.
2	Click **Realtime**.
3	Add the alarms that you want to print to a posted set. To add a log to a posted set, right-click on the desired log to display a drop-down menu. (You can right-click anywhere on the line of field information about the log.) Click **add to posted set** from the drop-down menu. Perform this step for all of the alarms that you want to print. **ATTENTION** The system will only print those alarms that you add to a posted set.
4	Click **Export posted records** (this button is located in the command bar, two buttons to the left of the Help button).
5	You will receive a prompt that asks if you want to export the posted set or the active records only. Choose your desired selection of **Active** or *Posted*. If you select **Active**, all the current active alarms will be exported. If you select **Posted**, only the alarms you have posted will be exported.
6	The **Export** window appears. The system displays a default file name and location to which the system will export the file. a. Browse through the path to folder you want to contain the file. b. Update the file name. c. Select a file format from the **Save as Type** pull-down menu. d. Click **Save**.
	—End—

View Logs

Viewing fault logs in Real-time

Step	Action

At the OAMP workstation

1 Click **Fault>log.**

2 Click the **Realtime** tab. In the **Realtime** window, select **Start**. Any new logs generated by the system will be displayed on the screen. Up to 100 logs will be displayed (default number). The **Realtime** Data window displays a list of logs with 16 fields for each log.

Field Name	Description
log-severity	A log category, such as log-info.
log-description	Description of the event that generated the log.
log-date-time	Date and time the log was recorded.
log-group-name	The subsystem that generated and identified the log.
log-number	A number the system assigns to the log. When paired with the group information, the number uniquely identifies each log.
shelf	Identification of the particular shelf generating the log.
slot	Identification of the slot generating the log.
system-node-name	The system node that generated the log.

3 To select a log and view it on the Administration panel, double-click anywhere on the log's row.

4 To stop the real-time display of logs, select **Stop** and no further logs will be displayed.

—End—

Modifying the number of logs displayed

Step	Action

At the OAMP workstation

1 Click **Fault>log**.

2 Click the **Realtime** tab. Click the box in the lower left hand corner of the window with the number. Select one of the following options which allows the system to display the corresponding numbers of logs selected:

- 100 (default)
- 200
- 500
- 1,000
- 2,000
- 5,000
- 10,000
- 100,000

3 After selecting from the drop-down list box options, click **Post** to apply your selection.

You can change the order of the alarms displayed by right-clicking on any column heading. When you right-click on a column heading, a pull-down menu appears with **"sort column ascending"** and **"sort column descending"** options. You can also change the order of the alarms by left-clicking on a column heading.

—End—

Begin a new log period

The system begins a new log collection period every 2,000 logs, or every six hours, or if there is a time of day change.

Starting or stopping a new log collection period manually

Step	Action

At the OAMP workstation

1 Click **Fault>log**.

2 Click the **Realtime** tab.

3 Click the **New period** command button.

4 Click the **Start** button.

5 To end the collection period, click **Stop**.

—End—

Adding and removing fields from Real-time data display

Step	Action
	At the OAMP workstation
1	Click **Fault>log**.
2	Click the **Realtime** tab.
3	Place the cursor over any of the column headings or column cells with information about logs, and then right-click on the selected area.
4	Click the customize option from the drop-down menu that appears. A **Columns** panel appears.
5	You can choose to display or remove a field from display by left-clicking on the box beside a field. A check beside a field name allows you to display a field. If you left-click on a check to remove it, then you are removing the field from display in the Realtime Data window. You may remove more than one item. The default displays all logs fields. When you highlight or select a field name from the Columns panel list, you can move the location of a field in the Realtime Data window. You can move a field toward the front or back of the column headings by left-clicking on the field name and the **Move Up** or **Move Down** button. You can move column headings by also left-clicking on a column heading and dragging it to the desired area. Your changes automatically appear in the Realtime Data window. They remain after you exit a session.

—End—

Performing a log search

Step	Action
	At the OAMP workstation
1	Click **Fault>log**.
2	Click the **Search** panel tab.

3 Left-click on the areas below the following criterion names to display pull-down menus: **Field**, **Condition**, **Value**, and **Records**. Click on the desired items to define your search.

For example, if you would like to display 100 current information logs, you would click **log severity** under the Field criterion name; on **equal** under the Condition criterion name; on **log-info** under the Value criterion name; and on **100** under the Records criterion name.

If you choose the **contains any** option from the Condition field list, you can provide more than one value in the in the Value field.

4 Click the **Retrieve** button, which is located in the upper right side of the Search window.

5 To perform another search that would display items in addition to the those displayed in a previous search, click the **Add** button. If the button is not already displayed, left-click on the arrow beside the area where you enter the Field criterion.

6 The criteria for the search already performed will appear in the small window below blank criteria boxes. Enter the desired values under the Field, Condition, Value and Records criterion names. Left-click on the **Retrieve** button.

7 You can also poll for new logs every minute by clicking on the auto-refresh check box at the bottom left of the Search screen.

Click the **Get Next** Button in the bottom of the Search window in order to retrieve a subsequent set of logs based on your search criteria. The default is to step through the logs in an interval of 100. You can change the default by choosing a value other than 100 in the Records field.

You can use the **Remove**, **Move Up** and **Move Down** buttons when you select a particular line of criteria beside these buttons.

You can display log details in the **Administration** tab. The **Administration** tab displays the log details in a structure different from the one in the **Search** window. In order to see a log in the **Administration** window, double-click on a line with log information in the **Search** window.

—End—

Exporting logs

Step	Action

At the OAMP workstation

1 Click **Fault>log**.

2 Click **Realtime** or **Search** depending on how you want to access the desired logs.

3 Add the logs that you want to print to a posted set. To add a log to a posted set, right-click on the desired log to display a drop-down menu. (You can right-click anywhere on the line of field information about the log.)

Click **add to posted set** from the drop-down menu. Perform this step for all of the logs that you want to print. Alternately, select several logs using your cursor and then click the **Post** button in the bottom right area of the log screen.

ATTENTION
The system will only print those logs that you add to a posted set.

4 Click **Export posted records** (this button is located in the command bar, two buttons to the left of the Help button).

5 You will receive a prompt that asks if you want to export the posted set. If you answer yes, only the alarms you have posted will be exported.

6 The Export window appears. The system displays a default file name and location to which the system will export the file.

a. Browse through the path to folder you want to contain the file.

b. Update the file name.

c. Select a file format from the **Save as Type** pull-down menu.

d. Click **Save**.

—End—

Retrieve Logs

Log display

To display logs in the **Realtime Data** window, complete the following procedure.

Displaying logs in the Realtime Data window

Step	Action
	At the OAMP workstation
1	Click **Fault>log**.
2	Click the **Administration** tab.
3	Click the **New period** command button.
4	Click the **Realtime** tab.
5	Click the **Start** button. You can also poll logs every minute by clicking on the auto-refresh check box.
	—End—

Begin a new log period

The system begins a new log collection period every 2,000 logs, or every six hours, or if there is a time of day change. To start or stop a new log collection period manually, complete the following procedure.

Starting or stopping a new log collection period manually

Step	Action
	At the OAMP workstation
1	Click **Fault>log**.
2	Click the **Administration** tab.
3	Click the **New period** command button.
4	Click the **Realtime** tab.
5	Click the **Start** button. You can also poll logs every minute by clicking on the auto-refresh check box.
6	To end the collection period, click **Stop**.

—End—

Test Links

Testing links

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.
2	Click the **Search** tab. Locate the link you want to test. Double-click the record to transfer it to the Administration panel.
3	Click **Test**.
4	Refer to the system logs for test results.
	—End—

CAM Shelf Fault Indicators

This section identifies the following LED indicator errors:

- LED(s) not illuminating
- LED(s) flashing

Front LEDs are not functioning

One or more LEDs are not lit on the front of the control Communications Applications Module (CAM) shelf or the extension CAM shelf.

Description

Unlit LED(s) on the front of a CAM shelf do not always indicate a problem. Front LEDs are not normally lit when the following conditions exist:

- card guides contain filler cards
- card guides contain SCSI Disk cards
- Real-time Controller (RTC), CAM Controller (CC), or application system nodes are in an offline state
- card guides contain no mission cards

LEDs that are not lit for the above do not require you to perform troubleshooting procedures. If you have determined that an LED for a mission card that should be lit is not lit, continue to the next section.

Corrective action

Determine whether any alarms were generated. Click **Fault>alarm**. If any alarms appear, refer to the appropriate troubleshooting procedure.

Malfunctioning rear LEDs

One or more LEDs are not lit on the back of a CAM shelf.

Description

Unlit LED(s) on the rear of a CAM shelf do not always indicate problems. Rear LEDs are not normally lit when the following conditions exist:

- card guides contain Filler transition modules (TMs)
- RTC, CC, or application system nodes are in an offline state
- card guides do not contain any TMs

LEDs that are not lit for the above do not require you to perform troubleshooting procedures.

If you have determined that an LED is not lit for a TM that should be lit, continue to the next section.

Corrective action

Determine whether any alarms were generated. Click Fault>alarm. If any alarms are displayed, refer to the appropriate troubleshooting procedure in this document.

Flashing LEDs

There are one or more LEDs flashing on the front of a CAM shelf

Description

Flashing green LEDs on the front of a CAM shelf indicate that the associated mission cards are enabled, but locked.

Corrective action

To troubleshoot this problem, perform the following procedure.

Unlocking the affected mission cards

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Right-click on the desired node. A drop-down menu appears. Click **Unlock**.

—End—

ATTENTION

There is another method to unlock an affected node. Double-click the affected RTC, CC or application system node in the Graphical View window. The Administration window, which includes associated provisioning and operational areas, appears. Click the **Unlock** option on the top bar in the Administration window. You will receive a Confirmation Required prompt. Click **Yes**.

Faults: AA1 Driver Alarms

AA1 Driver, 08: ATM Backplane failure (Minor)

Description

An asynchronous transfer mode (ATM) backplane failed. The system node does not receive duplicate messages.

If more than one alarm is received for each application system node on a shelf, a hardware problem in one of the CAM Controllers (CC) caused the alarm. If the alarm is on only one system node on a shelf, a hardware problem in that system node caused the alarm.

Corrective action

If a failure in a CC caused the problem, perform the corrective action in the Problem caused by CAM Controller (CC) section of this procedure. If a failure in a system node caused the alarm, perform the corrective action in the Problem caused by Link System Node section of this procedure.

Problem caused by CAM Controller (CC)

If the problem is caused by the CC, perform diagnostic tests on each CC to determine the CC that caused the alarm.

You can run diagnostic test by reloading the CC. If the CC reloads and works as expected, there are no problems on the CC. To run a diagnostic test on a CC system node, perform the following steps:

Running a diagnostic test on a CC system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click on the CC system node that you want to test.
4	Click **Lock** button to lock the CC system node.
5	Click **Load**. The CC system node boot image is downloaded and the CC system node is re-initialized and enabled. Observe the log and operational measurement (OM) systems to verify there are no indications of problems associated with this activity. You can observe the logs by clicking **Fault >log**.

You can observe OMs by clicking on **Performance>om** from the drop-down menu. Click the **Search** panel. In the Field criterion box, left-click **om-type**. Left-click **equals** in the Condition criterion box. Left-click on accumulate in the **Value** criterion box. Finally, left-click the **Retrieve** button.

If the test does not pass, replace the mission card and TM for the CC.

6 Click **Unlock** to return the card to service.

—End—

CAUTION
Wear wrist straps and use standard antistatic precautions.

Replacing the mission card and TM of the CC system node

Step	Action

At the OAMP workstation

1 While in the Administration window for the CC system node, click **Lock** if the CC is not already locked.

2 Click **Offline**.

3 Obtain a new mission card and transition module (TM), verify they have the correct PEC labels, and make sure the top and bottom latches are in the outward position.

ATTENTION
If the new mission card and TM have different PECs than the ones you are replacing, you must change the PEC in the Provisioning and Maintenance window before loading the card.

4 Before you replace a CC mission card, unseat its corresponding OC-3 TM. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors. Remove additional fiber-optic cables, if applicable.

5 Press outward on the top and bottom latches of the mission card or TM to release it from the CAM shelf. Two audible clicks can be heard when the mission card or TM is released completely.

6 Grasp the top and bottom latches of the mission card or TM and gently pull it toward you to remove it from the CAM shelf.

7 Position the top and bottom latches facing you, and gently slide the mission card into the card guide of the one you removed, seating the bottom and then the top of the mission card into the card guide.

8 Apply pressure to the faceplate near the latches until you feel resistance.

9 Snap the top and bottom latches of the mission card inward, toward one another. Two audible clicks can be heard when the mission card is seated properly.

10 Repeat steps 7 to 9 to replace the OC-3 TM.

11 After you reseat the OC-3 TM, plug in its connectors. Turn the thumbscrews on the top and bottom of the connectors to tighten the connectors.

12 On the front and rear of the appropriate CAM shelf, press Lamp Test. If the LEDs do not light for the system node you just replaced, make sure the mission card and TM are seated properly by unseating each and completing steps 4-11 again.

13 Wait for the LEDs to light. On the CC system node Administration window, click **Load** and wait for the system node to enable.

14 Click **Unlock**.

15 If the CC system node does not enable, or system logs or OMs indicate the problem persists, contact the next level of support.

—End—

Problem caused by link system node

If the problem is caused by a link system node, determine the link system node that caused the alarm.

CAUTION
Wear wrist straps and use standard antistatic precautions.

Replacing the mission card and TM of the affected link system node

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click **Graphical View**.

3 Double-click the slot of the desired system node.

4 Click **Lock**.

5 Click **Offline**.

6 Obtain a new mission card and TM, verify they have the correct PEC labels, and make sure the top and bottom latches are in the outward position.

ATTENTION

If you are replacing a V.35 TM, check the configuration of the DTE/DCE modules on the new TM card. For example, if the operational mode of a TM port is DTE, the operational mode at the remote site must be DCE.

For details on checking the configuration of a V.35 TM refer to "Verify the Operational Mode of Each V.35 TM Port" (page 185).

ATTENTION

If the new mission card and TM have different PECs than the ones you are replacing, you must change the PEC in the Provisioning and Maintenance window before loading the card.

7 Before you unseat the TM, remove the connector(s) attached to it by unscrewing the thumbscrews on the top and bottom of each connector. Gently pull off the cable connector(s).

8 Press outward on the top and bottom latches of the mission card or TM to release it from the CAM shelf. Two audible clicks can be heard when the mission card or TM is released completely.

9 Grasp the top and bottom latches of the mission card or TM and gently pull it toward you to remove it from the CAM shelf.

10 Position the top and bottom latches of the new mission card or TM facing you, and gently slide the mission card or TM into the card guide of the one you removed, seating the bottom of the mission card or TM into the card guide and then the top.

11 Apply pressure to the faceplate near the latches until you feel resistance.

12 Snap the top and bottom latches of the mission card or TM inward, toward one another. Two audible clicks can be heard when the mission card or TM is seated properly.

13 After you reseat the TM, plug in its TM connector(s). Turn the thumbscrews on the top and bottom of the connector(s) to tighten the connectors.

14 On the front and rear of the appropriate CAM shelf, press Lamp Test. If the LEDs do not light for the system node you just replaced, make sure the mission card and TM are seated properly by unseating each, and complete steps 3 to 13 again.

15 Wait for the LEDs to light.

If the Link system node does not enable, or system logs and OMs indicate the problem persists, contact your next level of support.

16 Click **Load** to return the system node to full service.

17 Click **Unlock**.

—End—

AA1 Driver, 09: CRC Err Count Threshold Reached (Critical, Major, Minor)

Description

The system generates this alarm when the CRC error count crosses the defined threshold value. The number of plane 1 or plane 2 CRC errors has exceeded the threshold value, indicating a possible inter-shelf messaging issue.

Corrective action

Contact your next level of support.

AA1 Driver, 10: Plane Msg Count Threshold Reached (Critical, Major, Minor)

Description

The system generates this alarm when the plane message count crosses the defined threshold value. The difference between the plane 1 message count and the plane 2 message count becomes greater than the threshold value, indicating a possible inter-shelf messaging issue.

Corrective action

Contact your next level of support.

AA1 Driver, 11: Raw Cell Count Threshold Reached (Critical, Major, Minor)

Description

The system generates this alarm when the raw cell count crosses the defined threshold value.

Corrective action

Contact your next level of support.

AA1 Driver, 12: Raw Msg Count Threshold Reached (Critical, Major, Minor)

Description

The system generates this alarm when the raw ATM message count crosses the defined threshold value.

Corrective action

Contact your next level of support.

AA1 Driver, 13: Seq. No. Reset Count Threshold Reached (Critical, Major, Minor)

Description

The system generates this alarm when the sequence number reset count crosses the defined threshold value. The number of times the system resets the sequence numbers, after receiving five consecutive duplicate cells, becomes greater than the threshold value.

Corrective action

Contact your next level of support.

ATM Driver Alarms

ATM Device Driver, 08: Physical Device Excessive Interrupts (Major)

Description

The asynchronous transfer mode (ATM) physical device on the CC card generated more than the normal number of interrupts to the processor. This is detrimental to system performance and can indicate a hardware failure.

Corrective action

To clear this alarm, perform the following procedures:

- "Reloading the CC system node" (page 27)
- "Reseating the CC system node card" (page 28)
- "Replacing the affected CC system node" (page 29)

Reloading the CC system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Click **Lock**.
5	Click **Load** and wait for the CC system node to enable.
6	Click **Unlock**. If the CC system node does not load or enable, or if the system brings up another Physical Device Excessive Interrupts alarm, proceed to the next section.

—End—

CAUTION
Wear wrist straps and use standard antistatic precautions.

Reseating the CC system node card

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Click **Lock**.
5	Click **Offline**.
6	Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the retaining screws on the top and bottom of the connectors. Gently pull off the cable connectors.
7	Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.
8	Grasp the top and bottom latches of the mission card. Gently pull it toward you to remove them from the CAM shelf.
9	Ensure the top and bottom latches are in the outward position by pressing outward on each latch.
10	Re-insert the card by positioning the top and bottom latches facing you. Gently slide the bottom of the mission card into the card guide first, then slide in the top.
11	Apply pressure to the faceplate until you feel resistance.
12	Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.
13	Repeat steps 10 to 12 to reseat the TM.
14	After you reseat the TM, plug in its connectors and turn the retaining screws on the top and bottom of the connectors to tighten them.
15	On the front and rear of the CAM shelf, press the **Lamp Test** buttons.
16	If the LEDs do not light, replace the mission card or TM of the affected CC system node.
17	Click **Load**. Wait for the system to enable. Click **Unlock**.

If the system does not clear the alarm, contact your next level of support.

18 Click **Unlock** to ensure the CC system node returns to full service. If the system node does not load, enable, or bring up the Physical Device Excessive Interrupts alarm, perform the steps in the next section. If the system node enables, this procedure is complete.

—End—

CAUTION
Wear wrist-straps and use standard antistatic precautions.

Replacing the affected CC system node

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click the **Graphical View** tab.

3 Double-click the slot of the desired system node.

4 Click **Lock**.

5 Click **Offline**.

6 Obtain a new mission card and TM; verify they have the correct PEC labels; and ensure the top and bottom latches are in the outward position.

ATTENTION
If the new mission card and TM have different PECs than the ones you are replacing, you must change the PEC in the Provisioning and Maintenance window before loading the card.

7 Unseat and disconnect the OC-3 TM for the CC mission card.

8 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

9 Grasp the top and bottom latches of the mission card. Gently pull it toward you to release it from the CAM shelf.

10 Ensure the top and bottom latches of the new card are in the outward position by pressing outward on each latch.

11 Position the top and bottom latches facing you. Gently slide the bottom of the new card into the card guide first, then slide in the top.

12 Apply pressure to the faceplate until you feel resistance.

13 Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

14 Repeat steps 7 to 11 to replace the TM.

15 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

16 On the front and rear of the CAM shelf, press the **Lamp Test** buttons.

17 If the LEDs do not light, replace the mission card or TM of the affected CC system node.

18 Click **Load** from the top bar of the platform - node window, and wait for the system to enable.

19 Click **Unlock** to ensure the CC system node returns to full service. If the system node does not enable, contact your next level of support. If the system node enables, this procedure is complete.

If the system does not clear the alarm, contact your next level of support.

—End—

Clearing Boot Alarms

Boot, 1: Boot Manager Hardware Mismatch (Minor)

Description

This alarm occurs when a mismatch is detected between a Real-time Controller (RTC), Communications Applications Module (CAM) Controller (CC), or application system node configuration and the actual mission cards and transition modules (TMs) that were installed for that system node.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- "Viewing the alarm" (page 31)
- "Replacing mission cards or TMs in system nodes" (page 176)

Viewing the alarm

Step	Action
	At the OAMP workstation
1	Determine whether the mission card or TM caused this alarm. To do this, click **Fault** from the main window to display a drop-down menu. Click **alarm** from the drop-down menu. The fault - alarm window appears.
2	On the fault - alarm window, review the lines of alarm information in the Realtime Data window. If the Realtime Data window is not already displayed, click the Realtime window to display it. If one of the following messages appears, perform procedure "Replacing mission cards or TMs in system nodes" (page 176). • installed AA module does not match config data • installed assembly does not match config data • installed base card does not match config data • TM does not match config data

—End—

Boot, 4: Boot Failure (Minor)

Description

This alarm indicates that loading of a system node (CC or application) was aborted because the system was unable to recover the system node within the maximum number of loading attempts.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- "Recover a CC System Node" (page 32)
- "Recover an application system node" (page 34)

Recover a CC System Node

To recover a CC system node, complete the following procedure(s), as necessary.

- "Loading the CC system node" (page 32)
- "Reseating cards in system nodes" (page 32)
- "Replacing mission cards or TMs in system nodes" (page 176).

Loading the CC system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Click **Lock**.
5	Click **Load**.

—End—

Reseating cards in system nodes

Step	Action
	At the OAMP workstation
1	If you are reseating cards and in a CC system node, ensure that node is offline. a. Click **Configuration>platform>node**. b. Click the **Graphical View tab.**

c. Double-click on the appropriate CC system node in the Graphical View window.

d. Click **Lock**.

e. Click **Offline**.

2 Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

3 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

4 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION

If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in "Verify the Operational Mode of Each V.35 TM Port" (page 185).

5 Ensure the top and bottom latches are in the outward position by pressing outward on each latch.

6 Position the top and bottom latches facing you, and gently slide the bottom of the mission card into the card guide first, then slide in the top.

7 Apply pressure to the faceplate until you feel resistance.

8 Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

9 Repeat steps 5 to 8 to reseat the TM.

10 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

11 On the front and rear of the CAM shelf, press the Lamp Test buttons.

12 If the LEDs do not light, replace the mission card or TM of the affected system node.

13 If you reseated the mission card and TM on the CC system node, click **Load** and wait for the system node to enable.

14 Click **Unlock** to ensure the system node returns to full service. If the system node does not enable, perform procedure "Replacing mission cards or TMs in system nodes" (page 176).

15 If the LEDs light, this procedure is complete.

—End—

Recover an application system node

To recover an application system node, complete the following procedures:

- "Enabling a CC system node" (page 34)
- "Loading an application system node" (page 35)
- "Reseating cards in system nodes" (page 35)
- "Replacing mission cards or TMs in system nodes" (page 176).
- "Verify the Operational Mode of Each V.35 TM Port" (page 185).

Enabling a CC system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click on the appropriate CC system node in the Graphical View window.
4	If **Enabled** appears in the Operational Data box, load the application system node, as described in the next section. If **Disabled** appears in the Operational State box, repeat steps 1 to 3 to determine if the other CC system node is enabled. If the other CC system node is enabled, load the application system node, as described in the next section. If both CC system nodes are disabled, recover a CC system node (described previously), and load the application system node, as described in the next section. If both CC system nodes were disabled and you just recovered one, the system automatically recovers all application system nodes that are not offline. You can wait several minutes for the application system nodes to recover and then view the fault - alarm window to determine whether all have recovered, or you can begin recovering the application system nodes immediately.

—End—

Loading an application system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click on the appropriate CC system node in the Graphical View window.
4	Click **Lock** if the application system node is not locked.
5	Click **Load** and wait for the application system node to enable.
6	Click **Unlock** to ensure the system node returns to full service. If the application system node does not return to full service, reseat the associated mission card and TM, as described in the next section.

—End—

Reseating cards in system nodes

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click on the appropriate CC system node in the Graphical View window.
4	Click **Lock**.
5	Click **Offline**.
6	Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

7 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

8 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION

If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in "Verify the Operational Mode of Each V.35 TM Port" (page 185).

9 Ensure the top and bottom latches are in the outward position by pressing outward on each latch.

10 Position the top and bottom latches facing you, and gently slide the bottom of the mission card into the card guide first. Then slide in the top.

11 Apply pressure to the faceplate until you feel resistance.

12 Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

13 Repeat steps 9 to 12 to reseat the TM.

14 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

15 On the front and rear of the CAM shelf, press the Lamp Test buttons.

16 If the LEDs do not light, replace the mission card or TM of the affected system node.

17 If you reseated the mission card and TM on the CC system node, click **Load** and wait for the system node to enable.

If the system node does not enable, replace the mission card and TM of the affected CC system node, perform procedure "Replacing mission cards or TMs in system nodes" (page 176).

18 Click **Unlock** to ensure the system node returns to full service.

19 If the LEDs light, this procedure is complete.

—End—

Buffer Manager Alarms

Buffer Manager, 5: xx percent of buffer_type control buffer in use more than x minutes (Minor)

Description

This alarm occurs when more than 75 percent of the specified control buffer (small or large) pool has been allocated for more than the specified buffer pool allocation time limit.

Corrective action

Reload the affected Real-time Controller (RTC) or application system node during the next scheduled maintenance window. Perform the following procedures:

- "Reloading the RTC system node" (page 37)
- "Loading a system node" (page 38)

Reloading the RTC system node

Step	Action
	At the OAMP workstation
1	Open the Administration window for the affected RTC system node. To do this, perform this following steps: a. Click **Configuration>platform>node**. b. Click the **Graphical View** tab. c. Double-click the slot of the desired system node.
2	If the affected system node is the active RTC system node, proceed to step 3. Otherwise, proceed to step 4.
	ATTENTION If this alarm is raised on the active RTC system node, and if the inactive RTC system node is enabled and unlocked , the system will perform a SWACT operation automatically.
3	Click **SWACT**.
4	If the RTC system node is locked, proceed to step 5. If the RTC system node is unlocked, click **Lock** and proceed to step 5.
5	Click **Load**.
6	Click **Unlock**.

If the alarm clears, the procedure is complete. If the alarm does not clear, contact your next level of support.

—End—

Loading a system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Click **Lock**.
5	Click **Load**.
6	If the affected system node was an IP link system node, determine if all application server processes (ASP) are back in service. If any ASPs are still out of service, follow the procedure "Activating the paths for each ASP" (page 49).
7	If the affected system node was an SS7 link system node, determine if all linksets are back in service. If any linksets are still out of service, follow the procedure "Activating the links in each linkset" (page 161).
8	If the system node does not return to full service, reseat the associated mission card and TM.

—End—

Buffer Manager, 6: xx percent of buffer_type control buffer in use more than x minutes (Major)

Description

This alarm occurs when more than 85 percent of the specified control buffer (small or large) pool has been allocated for more than the specified buffer pool allocation time limit.

Corrective action

Reload the affected RTC or application system node during the next scheduled maintenance window. Perform the following procedures:

- Reload the RTC system node, see "Reloading the RTC system node" (page 37).
- Load the system node, see "Loading a system node" (page 38).

Buffer Manager, 7: xx percent of buffer_type control buffer in use more than x minutes (Critical)

Description

This alarm occurs when more than 95 percent of the specified control buffer (small or large) pool has been allocated for more than the specified buffer pool allocation time limit.

Corrective action

Reload the affected RTC or application system node during the next scheduled maintenance window. Perform the following procedures:

- Reload the RTC system node, see "Reloading the RTC system node" (page 37).
- Load the system node, see "Loading a system node" (page 38).

Configuration Alarms

Configuration, 27: Data Boot Pointer Mismatch (Minor)

Description

The system generates this alarm when the boot data snapshot setting on a system node is changed to a value other than the value of the current running data snapshot.

Corrective action

This alarm normally occurs while you are restoring your system to a previously stored configuration. If this alarm has occurred while you are performing a restore operation, you can ignore this alarm and continue with your procedure. This alarm will be cleared when you have completed performing the restore procedure.

If a restore operation is not being performed when this alarm occurs, contact your next level of support.

Configuration, 28: Boot Image Mismatch (Minor)

Description

The system generates this alarm when the boot image file setting on a system node is changed to a value other than the current running image file.

Corrective action

Load the system node.

This procedure can be found in the USP Compact Maintenance Procedures section. If the alarm clears, the procedure is complete. If the alarm does not clear, contact your next level of support.

Configuration, 29: Missing Mate Node (Major)

Description

The system generates this log when only one of a mated-pair system node is found on the same shelf in the system.

Corrective action

Make sure there are even numbers (that is, 0 or 2) of the mated-pair system node provisioned on the same shelf in the system.

Configuration, 37: Running Image does not Match Mate (Minor)

Description

The configuration management subsystem generates this alarm when the running image on a system node does not match the image on the mate system node.

Corrective action

To clear this alarm, perform the following procedure.

Modifying the boot image

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Select the boot image for this system node from the **Boot Image** list.
5	Click **Modify**. A confirmation dialog box appears.
6	Click **Yes**.
7	Click **Lock** if the system node for which you changed the boot image is not locked.
8	Click **Load** and wait for the system node with the boot image change to enable.
9	Click **Unlock** to ensure the system node returns to full service. If the system node does not enable, contact your next level of support.

—End—

Data Audit Alarms

Data Audit, 1: Database is Corrupt (Minor)

Description

This alarm occurs when a database is corrupted on the specified RTC system node or application system node running SS7.

Corrective action

To clear this alarm, perform a load operation on the affected RTC or application system node running SS7.

Loading the RTC system node

Step	Action

At the OAMP workstation

1 Open the Administration window for the associated RTC system node. To do this, perform this following steps:

a. Click **Configuration>platform>node**.

b. Click the **Graphical View** tab.

c. Double-click the slot of the desired system node.

2 If the affected system node is the active RTC system node, proceed to step 3. Otherwise, proceed to step 4.

ATTENTION

If this alarm is raised on the active RTC system node, and if the inactive RTC system node is enabled and unlocked, the system will perform a SWACT operation automatically.

3 Click **SWACT**.

4 If the RTC system node is locked, proceed to step 5. If the RTC system node is unlocked, click **Lock** and proceed to step 5.

5 Click **Load**.

6 Click **Unlock**.

If the alarm clears, the procedure is complete. If the alarm does not clear, contact your next level of support.

—End—

Loading the application system node running SS7

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Click **Lock**.
5	Click **Load**.
6	Click **Unlock** to ensure the application system node returns to full service. If the alarm does not clear, contact your next level of support.

—End—

Data Audit, 2: RTC Sanity Threshold Reached (Critical, Major, Minor)

Description

The system generates this alarm when the RTC sanity count OM crosses the defined threshold value.

Corrective action

For assistance in clearing this alarm, contact your next level of support.

Database Synchronization Alarms

Database Sync, 13: NFS Mount Daemon Exited (Major)

Description

The Network File System (NFS) mount on one of the RTC system nodes has exited.

Corrective action

To clear the alarm, perform the following procedure.

Reloading the RTC system node

Step	Action

At the OAMP workstation

1 Open the Administration window for the associated RTC system node. To do this, perform this following steps:

a. Click **Configuration>platform>node**.

b. Click the **Graphical View** tab.

c. Double-click the slot of the desired system node.

2 If the affected system node is the active RTC system node, proceed to step 3. Otherwise, proceed to step 4.

ATTENTION

If this alarm is raised on the active RTC system node, and if the inactive RTC system node is enabled and unlocked, the system will perform a SWACT operation automatically.

3 Click **SWACT**.

4 If the RTC system node is locked, proceed to step 5. If the RTC system node is unlocked, click **Lock** and proceed to step 5.

5 Click **Load**.

6 Click **Unlock**.

If the alarm clears, the procedure is complete. If the alarm does not clear, contact your next level of support.

—End—

Disk Maintenance Alarms

Disk Maintenance, 4: SCSI Disk Free Space Low (Major)

Description

The SCSI Disk does not have enough free space available. This can cause degraded system performance. This alarm is caused by storing too many files on the SCSI Disk.

ATTENTION

The procedure required to correct this problem must be performed from your alternate boot server.

Corrective action

To clear this alarm, perform the following procedure.

Freeing SCSI disk space

Step	Action

At the alternate boot server

1 View the Alarms window. To do this, click **Fault>alarm**.

2 Access the File Manager window. To do this, click **Administration>file-manager**.

3 In the **Destination** list, select the RTC system node (RTC12 or RTC15) that generated this alarm.

4 In the **Snapshot** list, determine which snapshots you want to delete or backup.

To delete a snapshot, select the snapshot and click **Delete**.

To backup a snapshot to your alternate boot server:

a. In the Source list, select the drive on which you want to back up this snapshot.

b. In the Snapshot list, select the snapshot you want to back up and click Left Arrow.

To free enough disk space to allow this alarm to clear, you may need to delete or backup more than one snapshot.

5 After a couple of minutes, view the Alarms window again. If this alarm is still displayed, contact your next level of support.

—End—

Disk Maintenance, 5: Disk Formatting (Major)

Description

The system is formatting a disk. The information and data fields of the related log indicate the length of time the formatting can be expected to take.

Corrective action

You must wait for the disk formatting to finish before you can perform provisioning activities. The system clears this alarm automatically when the disk formatting is complete.

IPS7 Alarms

IPS7, 1: IPS7 Path Alarm (Critical, Major, Minor)

Each path to an application server process (ASP) failed. This alarm can be caused by the following:

- a disabled IP link system node (local or remote)
- cable and/or connection problems
- remote site problems

Corrective action

To clear this alarm, perform the following procedures, as necessary.

- Load all disabled IP link system nodes, see "Loading a system node" (page 47).
- Reseat the mission card and TM of the IP link system node, see "Reseating cards in system nodes" (page 48).
- Activate the paths to each ASP, see "Activating the paths for each ASP" (page 49).
- Review the logs for path failures, see "Reviewing the logs for ASP path failures" (page 50).
- Inspect cables and transmitter equipment, see "Inspecting the cables" (page 51).
- Verify the IP addresses and ports for the paths, see "Verifying the IP address and port" (page 51).
- Reboot the IP link system node, see "Rebooting the IP link system node" (page 52).
- Recover a CC system node, see the procedure in the section "Recover an application system node" (page 53).
- Replace the mission card and TM of the affected IP link system node, see "Replacing mission cards or TMs in system nodes" (page 176).

Loading a system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.

4 Click **Lock**.

5 Click **Load**.

6 If the affected system node was an IP link system node, determine if all ASPs are back in service. If any ASPs are still out of service, follow the procedure "Activating the paths for each ASP" (page 49).

7 If the affected system node was an SS7 link system node, determine if all linksets are back in service. If any linksets are still out of service, follow the procedure "Activating the links in each linkset" (page 161).

8 If the system node does not return to full service, reseat the associated mission card and TM.

—End—

Reseating cards in system nodes

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click the **Graphical View** tab.

3 Double-click the slot of the desired system node.

4 Click **Lock**.

5 Click **Offline**.

6 Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

7 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

8 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION

If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in "Verify the Operational Mode of Each V.35 TM Port" (page 185).

9 Ensure the top and bottom latches are in the outward position by pressing outward on each latch.

10 Position the top and bottom latches facing you, and gently slide the bottom of the mission card into the card guide first, then slide in the top.

11 Apply pressure to the faceplate until you feel resistance.

12 Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

13 Repeat steps 9 to 12 to reseat the TM.

14 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

15 On the front and rear of the CAM shelf, press the Lamp Test buttons.

16 If the LEDs do not light, replace the mission card or TM of the affected system node.

17 If you reseated the mission card and TM on the CC system node, click **Load** (in the CC system node Administration window), and wait for the system node to enable. Then click **Unlock** to ensure the system node returns to full service. (The Unlock button is in the top bar of the window.) If the system node does not enable, perform procedure "Replacing mission cards or TMs in system nodes" (page 176).

18 If the LEDs light, this procedure is complete.

—End—

Activating the paths for each ASP

Step	Action
	At the OAMP workstation
1	Identify the affected ASP in the Alarms window. Click **Fault>alarm**.
2	Click **Configuration> ips7>application-server-process-path**. All provisioned ASPs are listed in the asp-name field in the Provisioning Data box that appears.

3 Click on the name of the ASP you want to activate. All data relating to this ASP automatically appears. If you are unsure of the ASP name, scroll through the list.

4 Click the **Up** button in the top bar of the window to activate the paths in this ASP.

5 Monitor the ASP Path Status list to determine whether any paths in this ASP become active. Look in the Operational Data box in the Administration window to observe if the paths in the ASP become active.

If:	Do:
None of the paths become active	Continue this procedure at step 6.
Some of the paths become active	Go to "Reviewing the logs for ASP path failures" (page 50).
All the paths in the ASP become active	This procedure is complete.

6 Deactivate and activate this ASP (click the **Down** button in the top of the window. Wait several seconds, and then click the **Up** button).

7 Monitor the ASP Path State list to determine whether any paths in this ASP become active.

If:	Do:
All of the paths become active	This procedure is complete.
Some, or none, of the paths become active	Go to "Reviewing the logs for ASP path failures" (page 50).

—End—

Reviewing the logs for ASP path failures

Step	Action

At the OAMP workstation

1 Review the Logs for ASP Path Failures in the fault - log window. To access this fault log window, click **Fault>log** from the drop-down menu. The fault - log window appears.

2 In the Realtime Data window, identify all ASP path failure logs that correspond to the ASPs you tried to activate.

3 If any of the path failure information indicate a hardware problem, proceed to "Inspecting the cables" (page 51).

—End—

Inspecting the cables

Step	Action

At the USP chassis

1 Visually inspect all cables, repairing and replacing any bad cables. Complete the steps in the Activate the Paths for Each ASP section again. If the cables do not require repair or replacement, check the facilities at the remote site, correcting any problems, and complete the steps in the Activate the Paths for Each ASP section again. If problems are not reported at the remote site, proceed to "Verifying the IP address and port" (page 51).

—End—

Verifying the IP address and port

Step	Action

At the OAMP workstation

1 Call the remote site to verify that the IP address and port for each path on your USP matches the IP address and port settings on the remote site.

2 To view the IP address and ports assigned to a path, click **Configuration>ips7> application-server-process-path**.

3 Note the IP address and port displayed in the **IP Address** and **Port** boxes, respectively.

If:	Do:
The IP address and port of the path and the settings at the remote site do not match	Correct the settings and perform this procedure again, starting from the Enable all Disabled IP Link System Nodes section.
The IP addresses match	Continue this procedure.

4 Verify the transport protocol. If SCTP is chosen, configure one site as the client and the other site as the server.

—End—

Rebooting the IP link system node

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click the **Graphical View** tab.

3 Double-click the slot of the desired system node.

4 If **Enabled** appears in the **Operational Data** box, load the IP link system node, as described in steps 5 to 8.

If **Disabled** appears in the Operational Data box, repeat steps 1 to 4 to determine whether the other CC system node is enabled. If the other CC system node is enabled, load the IP link system node, as described in steps 5 to 8.

If both CC system nodes are disabled, proceed to the Recover a CC System Node section, and load the IP link system node, as described in steps 5 to 8.

If both CC system nodes were disabled and you just recovered one, the system automatically recovers all IP link system nodes that are not offline. You can wait several minutes for the IP link system nodes to recover and then view the fault-alarm window to determine whether all have recovered, or you can begin recovering the IP link system nodes immediately by completing steps 5 to 8. Access the fault-alarm window, by clicking on Fault from the main menu. and then selecting alarm from the drop-down menu.

5 In the **Graphical View** window, double-click the affected IP link system node. The Administration window for the IP link system node appears.

6 Click **Lock** if the IP link system node is not locked.

7 Click **Load**, and wait for the IP link system node to enable.

8 Click **Unlock** to ensure that it returns to full service. If the IP link system node does not enable, proceed to the procedure Replacing the mission card and TM of the affected link system node.

If the IP link system node enables but the IP paths do not recover, proceed to the procedure Replacing the mission card and TM of the affected link system node.

—End—

Recover an application system node

To recover an application system node, complete the following procedures:

- "Loading a system node" (page 53).
- "Reseating cards in system nodes" (page 53)
- "Replacing mission cards or TMs in system nodes" (page 176)
- "Verify the Operational Mode of Each V.35 TM Port" (page 185)

Loading a system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Click **Lock**.
5	Click **Load**.
6	If the affected system node was an IP link system node, determine if all ASPs are back in service. If any ASPs are still out of service, follow the procedure "Activating the paths for each ASP" (page 49).
7	If the affected system node was an SS7 link system node, determine if all linksets are back in service. If any linksets are still out of service, follow the procedure "Activating the links in each linkset" (page 161).

CAUTION
Wear wrist straps, and use standard antistatic precautions.

—End—

Reseating cards in system nodes

Step	Action

At the OAMP workstation

1 If you are reseating cards and in a CC system node, ensure that the node is offline.

a. Click **Configuration>platform>node**.

b. Click the **Graphical View** tab.

c. Double-click on the appropriate CC system node in the Graphical View window.

d. Click **Lock**.

e. Click **Offline**.

2 Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

3 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

4 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION

If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in the procedure Verifying the operational mode of each V.35 TM port.

5 Ensure the top and bottom latches are in the outward position by pressing outward on each latch.

6 Position the top and bottom latches facing you, and gently slide the bottom of the mission card into the card guide first, then slide in the top.

7 Apply pressure to the faceplate until you feel resistance.

8 Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

9 Repeat steps 5 to 8 to reseat the TM.

10 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

11 On the front and rear of the CAM shelf, press the Lamp Test buttons.

12 If the LEDs do not light, replace the mission card or TM of the affected system node.

13 If you reseated the mission card and TM on the CC system node, click **Load** and wait for the system node to enable.

14 Click **Unlock** to ensure the system node returns to full service. If the system node does not enable, replace the mission card and TM of the affected CC system node, as described in the procedure Replacing the mission card and TM in CC system nodes.

15 If the LEDs light, this procedure is complete.

—End—

IPS7, 8: AS Alarm (Critical)

A path to an application server (AS) failed as a result of the ASP being in a restoring state. This alarm can be caused by the following:

- a disabled IP link system node (local or remote)
- cable and/or connection problems
- remote site problems

Corrective action

To clear this alarm, do the following steps, as necessary.

- Load all disabled IP link system nodes, see "Loading a system node" (page 56).
- Reseat the mission card and TM of the IP link system node, see "Reseating cards in system nodes" (page 56).
- Activate the paths to each ASP, see "Activating the paths for each ASP" (page 49).
- Review the logs for path failures, see "Reviewing the logs for ASP path failures" (page 58).
- Inspect cables and transmitter equipment, see "Inspecting the cables" (page 58).
- Verify the IP addresses and ports for the paths, see "Verifying the IP address and port" (page 59).

- Reboot the IP link system node, see "Rebooting the IP link system node" (page 59).
- Recover a CC system node, see the procedures in the section "Recover an application system node" (page 60).
- Replace the mission card and TM of the affected IP link system node, see "Replacing mission cards or TMs in system nodes" (page 176).

Loading a system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot of the desired system node.
4	Click **Lock**.
5	Click **Load**.
6	If the affected system node was an IP link system node, determine if all ASPs are back in service. If any ASPs are still out of service, complete the procedure "Activating the paths for each ASP" (page 49).
7	If the affected system node was an SS7 link system node, determine if all linksets are back in service. If any linksets are still out of service, complete the procedure "Activating the links in each linkset" (page 161).

CAUTION
Wear wrist straps, and use standard antistatic precautions.

—End—

Reseating cards in system nodes

Step	Action
	At the OAMP workstation

1 If you are reseating cards and in a CC system node, ensure that node is offline.

   a. Click **Configuration>platform>node**.

   b. Click the **Graphical View** tab.

   c. Double-click on the appropriate CC system node in the Graphical View window.

   d. Click **Lock**.

   e. Click **Offline**.

2 Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

3 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

4 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION

If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in the procedure Verifying the operational mode of each V.35 TM port.

5 Ensure the top and bottom latches are in the outward position by pressing outward on each latch.

6 Position the top and bottom latches facing you, and gently slide the bottom of the mission card into the card guide first, then slide in the top.

7 Apply pressure to the faceplate until you feel resistance.

8 Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

9 Repeat steps 5 to 8 to reseat the TM.

10 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

11 On the front and rear of the CAM shelf, press the Lamp Test buttons.

12 If the LEDs do not light, replace the mission card or TM of the affected system node.

13 If you reseated the mission card and TM on the CC system node, click **Load** and wait for the system node to enable.

14 Click **Unlock** to ensure the system node returns to full service. If the system node does not enable, perform procedure "Replacing mission cards or TMs in system nodes" (page 176).

15 If the LEDs light, this procedure is complete.

—End—

Reviewing the logs for ASP path failures

Step	Action

At the OAMP workstation

1 Click **Fault>log**.

2 In the Realtime Data window, identify all ASP path failure logs that correspond to the ASPs you tried to activate.

3 If any of the path failure information indicate a hardware problem, proceed to the Inspect the Cables section.

—End—

Inspecting the cables

Step	Action

At the USP chassis

1 Visually inspect all cables, repairing and replacing any bad cables. Complete the steps in "Activating the paths for each ASP" (page 49) again. If the cables do not require repair or replacement, check the facilities at the remote site, correcting any problems, and complete the steps in "Activating the paths for each ASP" (page 49) again. If problems are not reported at the remote site, proceed to the "Verifying the IP address and port" (page 59).

—End—

Verifying the IP address and port

Step	Action

At the OAMP workstation

1 Call the remote site to verify that the IP address and port for each path on your USP matches the IP address and port settings on the remote site.

2 To view the IP address and ports assigned to a path, click **Configuration>ips7> application-server-process-path**.

3 Note the IP address and port displayed in the **IP Address** and **Port** boxes, respectively.

If:	Do:
The IP address and port of the path and the settings at the remote site do not match	Correct the settings and perform this procedure again, starting from the Enable all Disabled IP Link System Nodes section.
The IP addresses match	Continue this procedure.

4 Verify the transport protocol. If SCTP is chosen, configure one site as the client and the other site as the server.

—End—

Rebooting the IP link system node

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click the **Graphical View** tab.

3 Double-click the slot of the desired system node.

4 If **Enabled** appears in the **Operational Data** box, load the IP link system node, as described in steps 5 to 8.

If **Disabled** appears in the Operational Data box, repeat steps 1 to 4 to determine whether the other CC system node is enabled. If the other CC system node is enabled, load the IP link system node, as described in steps 5 to 8.

If both CC system nodes are disabled, proceed to the Recover a CC System Node section, and load the IP link system node, as described in steps 5 to 8.

If both CC system nodes were disabled and you just recovered one, the system automatically recovers all IP link system nodes that are not offline. You can wait several minutes for the IP link system nodes to recover and then view the fault-alarm window to determine whether all have recovered, or you can begin recovering the IP link system nodes immediately by completing steps 5 to 8. Access the fault-alarm window, by clicking on Fault from the main menu. and then selecting alarm from the drop-down menu.

5 In the **Graphical View** window, double-click the affected IP link system node. The Administration window for the IP link system node appears.

6 Click **Lock** if the IP link system node is not locked.

7 Click **Load**, and wait for the IP link system node to enable.

8 Click **Unlock** to ensure that it returns to full service. If the IP link system node does not enable, proceed to the procedure Replacing the mission card and TM of the affected link system node.

If the IP link system node enables but the IP paths do not recover, proceed to the procedure Replacing the mission card and TM of the affected link system node.

—End—

Recover an application system node

To recover an application system node, complete the following procedures:

- "Loading a system node" (page 60)
- "Reseating cards in system nodes" (page 61)
- "Replacing mission cards or TMs in system nodes" (page 176)
- "Verify the Operational Mode of Each V.35 TM Port" (page 185)

Loading a system node

Step	Action
At the OAMP workstation	
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.

3 Double-click the slot of the desired system node.

4 Click **Lock**.

5 Click **Load**.

6 If the affected system node was an IP link system node, determine if all ASPs are back in service. If any ASPs are still out of service, follow the procedure "Activate the Paths for Each ASP."

7 If the affected system node was an SS7 link system node, determine if all linksets are back in service. If any linksets are still out of service, follow the procedure "Activate the Links.

CAUTION
Wear wrist straps, and use standard antistatic precautions.

—End—

Reseating cards in system nodes

Step	Action

At the OAMP workstation

1 If you are reseating cards and in a CC system node, ensure that node is offline.

a. Click **Configuration>platform>node**.

b. Click the **Graphical View** tab.

c. Double-click on the appropriate CC system node in the Graphical View window.

d. Click **Lock**.

e. Click **Offline**.

2 Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

3 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

4 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION

If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in the procedure Verifying the operational mode of each V.35 TM port.

5 Ensure the top and bottom latches are in the outward position by pressing outward on each latch.

6 Position the top and bottom latches facing you, and gently slide the bottom of the mission card into the card guide first, then slide in the top.

7 Apply pressure to the faceplate until you feel resistance.

8 Snap the top and bottom latches of the mission card inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

9 Repeat steps 5 to 9 to reseat the TM.

10 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

11 On the front and rear of the CAM shelf, press the Lamp Test buttons.

12 If the LEDs do not light, replace the mission card or TM of the affected system node.

13 If you reseated the mission card and TM on the CC system node, click **Load** and wait for the system node to enable.

14 Click **Unlock** to ensure the system node returns to full service. If the system node does not enable, perform procedure "Replacing mission cards or TMs in system nodes" (page 176).

15 If the LEDs light, this procedure is complete.

—End—

IPS7, 9: AS Destination Deactivated Alarm (Minor)

Description

At least one AS destination is manually deactivated.

Corrective action

To clear this alarm, you must activate all AS destinations which were manually deactivated. Perform the following procedure.

Activating AS destinations

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-destination**.
2	Click the **Search** tab and then click **Retrieve** to locate the AS destination you want to activate.
3	Double-click on the routeset you want to activate to open it in the Administration panel.
4	Click **Activate**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.
	—End—

IPS7, 10: ASP Deactivated Alarm (Minor)

Description

At least one ASP is manually deactivated.

Corrective action

To clear this alarm, you must activate all ASPs which were manually deactivated. Perform the following procedure.

Activating ASPs

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-process**.
2	Click the **Search** tab and then click **Retrieve** to locate the ASP you want to activate.
3	Double-click on the ASP you want to activate to open it in the Administration panel.
4	Click **Activate**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.

—End—

IPS7, 11: ASP Path Deactivated Alarm (Minor)

Description

At least one ASP path is manually deactivated.

Corrective action

To clear this alarm, you must activate all ASP paths which were manually deactivated. Perform the procedure "Activating the paths for each ASP" (page 49).

Memory Facility Alarms

Memory Facility, 01: Low Memory Minor

Description

This alarm occurs when the amount of available memory has dropped to 400 Kilobytes or less. Simultaneous recovery of multiple system nodes may fail at this time.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- Log out unnecessary GUI connections.

  ATTENTION
  Logging off other users can only be performed from a user account with administrative privileges.

- Reload the affected RTC system node during a scheduled maintenance window.

Logging out unnecessary GUI connections

For more in formation about logging out users, see *USP Security and Administration* (NN10159-611).

Reloading the RTC system node

Step	Action
	At the OAMP Workstation
1	Open the associated Administration window for the affected RTC system node. To do this, perform the following steps: a. Click **Configuration>platform>node**. b. Click the **Graphical View** tab. c. Double-click the slot of the desired system node.
2	If the affected system node is the active RTC system node, proceed to step 3. Otherwise, proceed to step 4.

ATTENTION
If this alarm is raised on the active RTC system node, and if the inactive RTC system node is enabled and unlocked, the system will perform a SWACT operation automatically.

3 Click **SWACT**. When the switch of activity is complete, proceed to step 4.

4 If the RTC system node is locked, proceed to step 5. If the RTC system node is unlocked, click **Lock**, and proceed to step 5.

5 Click **Load** to download the boot image, and re-initialize and enable the RTC system node. (The Load button is located in the top bar of the window.)

6 When the load operation is complete, click **Unlock** to unlock the RTC system node.

ATTENTION
If the alarm clears, the procedure is complete. If the alarm does not clear, contact your next level of support.

—End—

Memory Facility, 02: Low Memory Major

Description

This alarm occurs when the amount of available memory has dropped to 200 Kilobytes or less. Simultaneous recovery of multiple system nodes may fail at this time. Multiple GUI connections may not be possible at this time.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- Log out unnecessary GUI connections, see "Logging out unnecessary GUI connections" (page 65).
- Reload the affected RTC system node now or during a scheduled maintenance window, see "Reloading the RTC system node" (page 65).

Memory Facility, 03: Low Memory Critical

Description

This alarm occurs when the amount of available memory has dropped to 100 Kilobytes or less, or when the largest block of contiguous memory has dropped below 40 Kilobytes. A new GUI connection attempt while this alarm is in effect can cause the RTC system node to fail.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- Log out unnecessary GUI connections, see "Logging out unnecessary GUI connections" (page 65).

- Reload the affected RTC system node immediately, see "Reloading the RTC system node" (page 65).

MTP Level 3 Event Alarms

MTP Level 3 Event, 17: Link Alarm (Critical, Major, Minor)

Each SS7 link within a combined linkset failed. This alarm can be caused by the following:

- a disabled SS7 Link system node (local or remote)
- cable and/or connection problems
- remote site problems

Corrective action

To clear this alarm, perform the following procedures, as necessary.

- Load all disabled SS7 link system nodes, see "Loading a system node" (page 69).
- Reseat the mission card and TM of the SS7 link system node, see "Reseating cards in system nodes" (page 70).
- Verify the Operational Mode of each V.35 TM port, see "Verify the Operational Mode of Each V.35 TM Port" (page 185).
- Activate links in each linkset, see "Activating the links in each linkset" (page 161).
- Review the logs for link failures, see "Reviewing the logs for link failures" (page 183).
- Verify all signal link testing (SLT) settings, see "Verifying all signal link test (SLT) settings" (page 71).
- Inspect cables and transmitter equipment, see "Inspecting cables and transmitter equipment" (page 71).
- Verify the PCs (local and remote), see "Verifying the point codes (PCs) (local and remote)" (page 72).
- Verify the SLCs, see "Verifying the signal link codes (SLCs)" (page 72).
- Perform BERT, see *USP Security and Administration* (NN10159-611).
- Reboot the SS7 link system node, see "Rebooting the SS7 link system node" (page 73).
- Recover a CC system node, see "Recovering a CC system node" (page 74).
- Replace the mission card and TM of the affected SS7 link system node, see "Replacing mission cards or TMs in system nodes" (page 176).

CAUTION
Wear wrist straps and use standard antistatic precautions.

Loading a system node

Step	Action

At the OAMP workstation

1 Open the affected system shelf window. To do this, click **Configuration>platform>node**.

2 To view the CAM shelf icon, click **Graphical View**.

3 Double-click the icon for the affected system node. The Administration panel appears.

4 If the system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

5 Click **Load**. Wait for the system node to enable and click **Unlock** (with confirmation) to ensure the system node returns to full service.

6 If the affected system node was an SS7 IP link system node, determine if all linksets are back in service. If any linksets are still out of service, perform procedure, "Activating the links in each linkset" (page 161).

7 If the affected system node was an SS7 link system node, determine if all linksets are back in service. If any linksets are still out of service, Activate the links. See the Configuration guide for more information.

8 If the system node does not return to full service, perform "Reseating cards in system nodes" (page 70) and repeat this procedure.

—End—

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Reseating cards in system nodes

Step	Action

At the OAMP workstation

1 Open the affected system shelf window. To do this, click **Configuration>platform>node**.

2 To view the CAM shelf icon, click **Graphical View**.

3 Double-click the icon for the intended CC system node. The Administration panel appears.

If the CC system node is:	Do:
Online	step 4.
Offline	step 6.

4 If the CC system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

5 Click **Offline**. At the confirmation prompt, click **Yes**.

6 Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

7 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

8 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION
If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in the procedure Verifying the operational mode of each V.35 TM port.

9 Ensure the top and bottom latches of the mission card or TM are in the outward position by pressing outward on each latch.

10 Position the top and bottom latches facing you of the mission card or TM, and gently slide the bottom of the card into the card guide first, then slide in the top.

11 Apply pressure to the faceplate until you feel resistance.

12 Snap the top and bottom latches of the mission card or TM inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

13 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

14 On the front and rear of the CAM shelf, press the Lamp Test buttons.

15 If the LEDs do not light, replace the mission card or TM of the affected system node.

16 If you reseated the mission card and TM on the CC system node, click **Load** (in the CC system node Administration view) and wait for the system node to enable. Then click **Unlock** to ensure the system node returns to full service. If the system node does not enable, replace the mission card and TM of the affected CC system node, as described in the procedure Replacing the mission card and TM of the affected CC system node.

17 If the LEDs light, this procedure is complete.

—End—

Verifying all signal link test (SLT) settings

Step	Action
	At the OAMP workstation
1	Determine whether an SLT failed for any links. To do this, click **Fault>log**. The Logs window appears.
2	If SLTs passed, proceed to "Inspecting cables and transmitter equipment" (page 71). If SLTs failed, proceed to the Check the GWS Mode section.

—End—

Inspecting cables and transmitter equipment

Visually inspect all cables, repairing and replacing any bad cables, and complete the procedure "Activating the links in each linkset" (page 161). If the cables do not require repair or replacement, check the facilities at the remote site, correcting any problems, and complete the procedure

"Activating the links in each linkset" (page 161)again. If problems are not reported at the remote site, proceed to the procedure "Verifying the point codes (PCs) (local and remote)" (page 72).

Verifying the point codes (PCs) (local and remote)

Step	Action

At the OAMP workstation

1 Call the remote site to verify that the PC on your USP matches the PC on the remote site.

2 Click **Configuration>mtp>system-id** to access the System Identity window.

3 Note the PC displayed in the Point Code box.

If:	Do:
The PCs of the remote office and your USP do not match	Correct the point code and return to the Enabling System Nodes section.
The PCs match	Proceed to the "Verifying the signal link codes (SLCs)" (page 72) procedure.

—End—

Verifying the signal link codes (SLCs)

Step	Action

At the OAMP workstation

1 Verify that the SLCs on your USP match those of the remote site. To do this, click **Configuration>mtp>linkset**. The SS7 MTP Linkset Administration window appears.

2 View the Linkset Status/Actions portion of the MTP Linkset Administration window, verifying that the SLCs set up for your USP match those of the remote site.

3 If the SLCs do not match, correct and perform this procedure again, starting from the Enable all Disabled SS7 Link System Nodes section.

If the SLCs match, check the facilities at the remote site, correcting any problems, and perform this procedure again, starting from the procedure Loading system nodes. If problems are not reported at the remote site, proceed to the Perform BERT section in *USP Security and Administration* (NN10159-6110.

—End—

Rebooting the SS7 link system node

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node**.
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click a CC system node. The CC system node provisioning and maintenance window appears. If Enabled appears in the Operational State box, load the SS7 link system node, as described in step 4 through step 6. If Disabled appears in the Operational State box, return to the Graphical View and double-click on the other CC system node is enabled. If the other CC system node to see if it is enabled and load the SS7 link system node, as described in step 4 through step 6. If both CC system nodes are disabled, proceed to the procedures to "Recovering a CC system node" (page 74), and load the SS7 link system node, as described in step 4 through step 6. If both CC system nodes were disabled and you just recovered one, the system automatically recovers all SS7 link system nodes that are not offline. You can wait several minutes for the SS7 link system nodes to recover and then view the Alarms window to determine whether all have recovered, or you can begin recovering the SS7 link system nodes immediately by completing step 4 through step 6.
4	From the Graphical View, double-click the affected SS7 link system node. The IP link system node provisioning and maintenance window appears.
5	Click **Lock** if the SS7 link system node is not locked.
6	Click **Load** and wait for the SS7 link system node to enable and click **Unlock** to ensure that it returns to full service. If it does not enable, or if the SS7 link system node enables but the IP paths do

not recover, proceed to the procedure "Replacing mission cards or TMs in system nodes" (page 176).

—End—

Recover a CC system node

Perform this set of procedures to remove MTP Level 3 Event, 17: Link Alarm (Critical, Major, Minor) alarm conditions.

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Recovering a CC system node

Step	Action
	At the OAMP workstation
1	Perform the procedure entitled "Loading a system node" (page 69) and load the CC system node.
2	As instructed in the loading procedure, if the CC system node does not return to full service, perform the procedure entitled "Reseating cards in system nodes" (page 70) for the mission card and TM of the CC system node.
3	Perform the procedure "Replacing mission cards or TMs in system nodes" (page 176).

—End—

MTP Level 3 Event, 39: Routeset Alarm (Critical, Major, Minor)

Critical alarm description

A routeset destination is inaccessible and there is at least one activated linkset to that destination.

ATTENTION

A linkset is not deactivated until a deactivate linkset operation is performed. Therefore you can deactivate all links at the link level but the linkset will still be activated.

If you deactivate the last in-service link on a linkset, you will receive a warning message which indicates your actions may impact network traffic.

Major alarm description

This alarm indicates one of the following:

- A routeset destination is restricted because there is a problem with the primary route. If the primary routeset is made up of a non-combined linkset, then all links in the linkset have failed. If the primary routeset is made up of a combined linkset, then one or both of the linksets that make up the combined linkset failed.
- A routeset destination is accessible but there are problems with one or all alternate routes. If the alternate route is made up of a non-combined linkset, then all links on that linkset have failed. If the alternate route is a combined linkset, then both linksets that make up the combined linkset failed.
- The alarm is the result of networking problems: one or more, but not all, of the routes does not have a Route Status of TFA.

ATTENTION

A linkset is not deactivated until a deactivate linkset operation is performed. Therefore you can deactivate all links at the link level but the linkset will still be activated.

If you deactivate the last in-service link on a linkset, you will receive a warning message which indicates your actions may impact network traffic.

Minor alarm description

A routeset destination is accessible but:

- The routeset destination is inaccessible by manually deactivating all linksets to that destination. In this case, a minor alarm is raised on USP but a critical alarm is raised on the Core because of the inaccessible routeset.
- The routeset contains an activated linkset and has one or more (but not all) activated links that are out of service.
- The routeset contains a combined linkset provisioned as an alternate route that has one activated linkset with all links active, but the links belonging to the other activated linkset all failed.

ATTENTION

A linkset is not deactivated until a deactivate linkset operation is performed. Therefore you can deactivate all links at the link level but the linkset will still be activated.

If you deactivate the last in-service link on a linkset, you will receive a warning message which indicates your actions may impact network traffic.

Corrective action

The following corrective action is required to clear this alarm:

- Determine which alarms are caused by network problems (these alarms cannot be resolved on the local system).
- Resolve all SS7 link alarms against failed links.

Determining which alarms are caused by network problems

Step Action

At the OAMP workstation

1 Open the affected system shelf window. To do this, click **Configuration>mtp>routeset**.

2 To view a list of major routset alarms, click **Search** and provide the following criteria.

Criteria	Selection
Field	alarm-status
Condition	equal
Value	major
Records	100

3 Click **Retrieve**.

4 If the Route Status is not TFA, then this alarm is the result of network problems and local maintenance is not appropriate.

Contact the far end office and notify them of the routeset alarm. If the problem is not resolvable, contact your next level of support.

5 If all routes have a Route Status of TFA and their Accessibility Status is "Inaccessible", go to the next procedure "Resolving all SS7 link alarms against failed links" (page 76).

—End—

Resolving all SS7 link alarms against failed links

Step Action

At the OAMP workstation

1 Access the SS7 MTP Linkset Administration window. To do this, click **Configuration>mtp>linkset**.

2 To view a specific linkset, click **Search** and provide the following criteria.

Criteria	Selection
Field	linkset-name[1]
Condition	equal
Value	<the linkset name>
Records	100

1. If the linkset name is not known, either choose another Field or modify the Condition and Value criteria.

3 Click **Retrieve**.

4 For the Inaccessible routeset(s), note all linksets and combined linksets provisioned as routes against the routeset. If there are no combined linksets, proceed to step 7.

5 Access the SS7 MTP Combined Linkset Administration window, linksets that make up the combined linkset are listed. To do this, click **Configuration>mtp>combined-linkset**. Make note of linksets that are provisioned as part of the combined linkset associated with the alarm.

6 Click **Search** and complete the necessary criteria to locate the combined linkset. Click **Retrieve** to locate.

7 At the SS7 MTP Linkset Administration window opened in step 1, find the links that make up the linksets and combined linksets noted in the previous steps.

8 Resolve all SS7 link alarms against these links by following the procedures under:

- MTP Level 3 Event, 17: Link Alarm (Critical)
- MTP Level 3 Event, 17: Link Alarm (Major)
- MTP Level 3 Event, 17: Link Alarm (Minor)

—End—

MTP Level 3 Event, 45: Link Utilization Threshold Reached (Critical, Major, Minor)

Description

The system generates this alarm when the link utilization OM crosses the defined threshold value.

The number of links in the linkset is not sufficient to handle the traffic on the linkset.

Corrective action

To clear this alarm, add more links to the linkset. To do this, perform the following procedure.

Provisioning links

Step	Action
	At the OAMP workstation
1	Access the SS7 MTP Link Administration window. To do this, click **Configuration>mtp>link** and complete the provisioning data.
2	Click the **link-type** arrow for a link type list and select the appropriate choice.
3	Click the **system-id** arrow for a system Identity list and select the system identity to be associated with this link.
4	Click the **linkset-name** arrow for linkset list and select a linkset.
5	At **slc** assign an unused SLC for this link. This code is a logical representation (0 through 15) of a physical link and is agreed upon with the far end code. The SLC is externally visible to the network. An SLC can only be used once per linkset. You can provision the following: • up to 48 linksets on a single-shelf system (control CAM shelf only) • up to 112 links on a dual-shelf system (control CAM shelf and extension CAM shelf) • up to 176 links on a three-shelf system (control CAM shelf and two extension shelves) • up to 240 links on a four-shelf system (control CAM shelf and three extension shelves) • up to 480 links on a five-shelf system (control CAM shelf and four extension shelves)

- up to 752 links on an eight-shelf system (control CAM shelf and seven extension shelves)

6 From the **shelf** menu, click on the ... box to view a list of platform nodes. Select the appropriate shelf by clicking on the shelf to highlight and then click **Select**. The shelf and slot automatically update.

7 Click **Add**.

8 Select an unused configured SS7 Link system node from the Node Name list. If you choose a used SS7 Link system node, the system notifies you with a message. The Link Speed, Interface, and Operational Mode boxes are updated based on your selection.

9 At **port** choose an unused port (0 through 3). If you choose a used port, the system notifies you with an information message when you add the link in.

10 Click the **SCTP Parm Index** list and select an SCTP parameter index number to associate with this link.

11 In the **Local Port** box, enter the number of the local, or server, port.

12 In the **Remote Port** box, enter the number of the remote, or client, port.

13 Click the **Operational Method** list and select an operation for the link. If you select "Server", the link initiates traffic. If you select "Client", the link accepts traffic from another link.

14 Determine the type of link that you are adding.

If:	Do:
you are provisioning a Channelized E1 Link	step 16.
you are provisioning an ATM High Speed Link	step 15.
you are provisioning any other link type	step 17.

15 For ATM High-speed Links, complete the following steps:

a. Select an ATM_VPI from the ATM_VPI list. The default is 0.

b. Select an ATM_VCI from the ATM_VCI list. The default is 5.

c. Select a SAAL parameter index from the SAAL Parm list.

There is no default SAAL parameter index.

d. Select a SAAL timer index from the SAAL Timer list.

There is no default SAAL timer index.

e. Proceed to step 16.

16 To provision a Channelized E1 Link, select a channel from the **Channel Selection** list.

17 Indicate whether the system should perform preventive cyclic retransmission (PCR) on the link using the **PCR** check box. PCR is recommended for all satellite links, and intercontinental links where the one-way propagation delay is greater than 15 ms. Both the transmitting and receiving terminal units of the link must use the same error correction method. If you enable PCR, proceed to step 18. Otherwise, proceed to step 20.

ATTENTION

PCR is not supported for ATM High Speed Links.

The default value is unchecked. If PCR is not enabled, the link will use basic error correction at MTP level 2.

18 Select a value between 5 and 20 (representing tenths of a second) in the **T7** box. This value represents the excessive delay of acknowledgement timer. PCR continually re-transmits unacknowledged message signaling units (MSU) until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

The default value for the T7 timer is 8, or 800 ms.

Changing the T7 timer value on this screen will not change the T7 timer value for the provisioned timer index. If PCR is selected, the value in the T7 timer box is used for the excessive delay of acknowledgement. If PCR is not selected, the value for T7 in the timer index is used for the excessive delay of acknowledgement.

19 Select a value between 1 and 50 (representing tenths of a second) in the **Roundtrip Delay** box. This value represents the round trip propagation delay for the link in milliseconds.

The default value is 10, or 1000 ms.

20 Indicate whether the system should periodically perform signal link testing (SLT). Click the **Periodic SLT** check box to change the test status (defaults to unchecked, no test).

Click the check box to toggle between checked and unchecked.

21 For ATM High-speed links, proceed to step 20. For all other link types, proceed to step 18.

22 Select a provisioned MTP link timer index from the **Level 2 Index** list.

The default index is the first available index, or index 0 if no indices have been provisioned.

23 Select a provisioned MTP link SLT timer index from the **SLT Index** list.

The default index is the first available index, or index 0 if no indices have been provisioned.

24 Click **Apply** to add the new link. The information for the link is added to the Link Records list.

—End—

MTP Level 3 Event, 48: Routeset Deactivated Alarm (Minor)

Description

At least one routeset is manually deactivated.

Corrective action

To clear this alarm, activate all the routesets which were manually deactivated.

Activating routesets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>routeset**.
2	Click the **Search** panel tab, click the **Retrieve** button, and locate the record you want to activate. Double-click the routeset to open it in the Administration panel.
3	Click **Activate**. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.

—End—

MTP Level 3 Event, 49: Linkset Deactivated Alarm (Minor)

Description

At least one linkset is manually deactivated.

Corrective action

To clear this alarm, activate all the linksets which were manually deactivated.

Activating linksets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>linkset**.
2	Click the **Search** panel tab, click the **Retrieve** button, and locate the linkset you want to activate. Double-click the linkset in the search results to transfer to the Administration panel.
3	Click **Activate** to activate the displayed linkset. All links in a linkset are activated by this command. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.

—End—

MTP Level 3 Event, 50: Link Deactivated Alarm (Minor)

Description

At least one link is manually deactivated.

Corrective action

To clear this alarm, activate all the links which were manually deactivated.

Activating links

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.
2	Click the **Search** panel tab, click the **Retrieve** button, and locate the record you want to activate. Double-click the link to open it in the Administration panel.
3	Click **Activate** to activate the displayed link. A confirmation dialog box appears When you activate a link, several boxes are updated in the Operational Date section of this window.
4	Click **Yes** to confirm the change.

—End—

SS7 IP High Speed Link Alarms

SS7 IP High Speed Link Alarms

Each SS7 IP High Speed link within a combined linkset failed. This alarm can be caused by the following:

- a disabled SS7 Link system node (local or remote)
- cable and/or connection problems
- remote site problems

Corrective action

To clear this alarm, perform the following procedures, as necessary.

- Activate SS7 IP High Speed links, see "Activating a link" (page 159)
- Activate SS7 IP High Speed links in each linkset, see "Activating the links in each linkset" (page 161)
- Review the logs for SS7 IP High Speed link failures, see "Reviewing the logs for link failures" (page 183)
- Inspect cables, see "Inspecting the cables for SS7 IP High Speed Link failures" (page 84)
- Verify the IP addresses and ports for the SS7 IP High Speed links, see "Verifying the IP address and port for SS7 IP High Speed Link failures" (page 85)
- Reboot the IP link system node, see "Rebooting the link system node" (page 164)

Inspecting the cables for SS7 IP High Speed Link failures

Step	Action
	At the USP chassis
1	Visually inspect all cables, repairing and replacing any bad cables. Perform procedure, "Activating the links in each linkset" (page 161). If cables do not require repair or replacement check the facilities at the remote side, correct any problems, and perform procedure, "Activating the links in each linkset" (page 161) again. If problems are not reported at the remote site, perform procedure, "Verifying the IP address and port for SS7 IP High Speed Link failures" (page 85)

—End—

Verifying the IP address and port for SS7 IP High Speed Link failures

Step	Action

At the OAMP workstation

1 Call the remote site to verify that the IP address and port for each path on your USP matches the IP address and port settings on the remote site.

2 To view the IP address and ports assigned to a path, click **Configuration>mtp>link**.

3 Note the IP address and port displayed in the **IP Address** and **Port** textboxes, respectively.

If	Do
The IP address and port of the path and the settings at the remote site do not match	Correct the setting and perform this procedure again. Confirm that all SS7 IP Link System Nodes are enabled and unlocked. See section, "System Node Maintenance Alarms" (page 102).
The IP addresses match	Continue this procedure.

4 Verify the transport protocol.

In **Configuration>mtp>link**, configure one site as the sctp-opreation-mode and the other site as the client.

In **Configuration>mtp>linkset**, if protocol-type is m3ua, configure the ipsp-type site as the client and the other site as the server.

5 If the IP addresses match, perform procedure, "Rebooting the link system node" (page 164).

—End—

SS7 IP High Speed Link Deactivated Alarms

Description

At least one link is deactivated.

Corrective action

To clear this alarm, activate all the links that were manually deactivated. Perform the following procedures, as necessary.

- Activate SS7 IP High Speed links, see "Activating a link" (page 159)

- Activate SS7 IP High Speed links in each linkset, see "Activating the links in each linkset" (page 161)
- Review the logs for SS7 IP High Speed link failures, see "Reviewing the logs for link failures" (page 183)
- Inspect cables, see "Inspecting the cables for SS7 IP High Speed Link failures" (page 84)
- Verify the IP addresses and ports for the SS7 IP High Speed links, see "Verifying the IP address and port for SS7 IP High Speed Link failures" (page 85)
- Reboot the IP link system node, see "Rebooting the link system node" (page 164)

Network Alarms

Network, 0: Connectivity State Change (Critical, Major, Minor)

Description

The alarm-clearing procedure is the same for all levels of severity for this alarm.

Connectivity has been lost between the RTC system nodes and the specified device on your system's LAN.

This alarm can be caused by the following:

- Cables to the specified device are improperly connected or damaged.
- The IP address of the specified device is incorrect.
- The specified device is powered off or faulty.

Corrective action

To clear the alarm, perform the following procedure.

Clearing: Connectivity State Change

Step	Action
	At the OAMP workstation
1	Determine if any cables from the device to the LAN are disconnected or damaged. If any cables are disconnected or damaged, reconnect or replace them.
2	Ensure that the IP address of your device is correct. To do this, refer to the CLI Interface specification for more information.
3	Ensure that the device is powered on.
4	Repair or replace the device.

—End—

Network, 3: No Response to Bootp Request (Major)

Description

The RTC did not receive a response to the bootp request within the 10 second timeout window.

This alarm can have one of the following causes:

- The bootp server is not running.
- The bootp server is not configured with the RTC MAC address.

- If the bootp server and the system are not on the same subnet, bootp forwarding may not be configured on the intermediate routers.

Corrective action

To clear this alarm, perform the following procedures as necessary:

- Verify that the bootp server is running.
- Verify that the RTC MAC address is correctly configured.
- Verify that the bootp forwarding is configured on intermediate routers.

For information on performing the corrective actions, refer to the bootp manuals.

Network, 4: Unable to Ping to Alt-Boot-Srv (Major)

Description

The RTC was not able to successfully ping the alternate boot server's IP address.

This alarm has one of the following causes:

- The bootp server has an incorrect IP address for the alternate boot server.

ATTENTION
If the system is using the bootp server shipped with the system, it has a fixed IP address. In this case, an incorrect IP address is not the cause of the alarm.

- The alternate boot server and system have a connectivity issue.

Corrective action

To clear this alarm, perform the following procedures as necessary:

- Verify that the bootp server is configured with the correct IP address for the alternate boot server.
- Verify that there are no network connectivity issues between the system and the alternate boot server.

For information on performing the corrective actions, refer to the bootp manuals.

Network, 5: Unable to FTP to Alt-Boot-Srv (Major)

Description

The RTC cannot establish an FTP connection to the alternate boot server's IP address using the internal identification and password.

This alarm has one of the following causes:

- The FTP server is not active.
- The user identification and password is not set up on the FTP server.

Corrective action

Perform the following procedures as necessary:

- Verify that the FTP server is running.
- Verify that the user identification and password is set up on the FTP server.

For information on performing the corrective actions, refer to the information on FTP in your server manuals.

Network, 6: Unable to NFS Mount Alt-Boot-Srv (Major)

Description

The RTC was not able to establish an NFS mount to the alternate boot server's IP address.

This alarm has one of the following causes:

- The NFS server is not active.
- The user identification and password is not setup on the NFS server.

Corrective action

Contact your next level of support.

Network, 7: Unable to Locate RTC boot (Major)

Description

The system cannot locate the RTC boot file included in the bootp response message.

This alarm has one of the following causes:

- The FTP server is not exporting the directory that contains the RTC boot file.
- The bootp server is configured with the wrong RTC boot load location.
- The RTC boot file was deleted.

Corrective action

To clear this alarm, perform the following procedures as necessary:

- Verify that the FTP server is exporting the directory that contains the rtcboot file.

- Verify that the bootp server is configured with the correct rtcboot file location.

If the alarm is not caused by one of the previous issues, verify that the rtcboot file exists on the alternate boot server.

For information on performing the corrective actions, refer to the information on FTP or bootp in your server manuals.

If this alarm is caused as a result of a missing rtcboot file on the alternate boot server, reset the alternate boot server configuration. To reset the alternate boot server information using the GUI, perform the following procedure.

Resetting the alternate boot server configuration

Step	Action
	At the OAMP workstation
1	Open the Alternate Boot Server window. To do this, click **Administration>alternate-boot-server**.
2	In the ABS Loads portion of the window, select the correct load name in the **rtc-12-loadname** list.
3	In the ABS Loads portion of the window, select the correct load name in the **rtc-15-loadname** list.
4	In the ABS Snapshot portion of the window, select the latest version of the data snapshot. The Description, Version, and Date boxes are updated automatically with the information about the snapshot.
5	Click **Modify** to change the site.

—End—

Network, 8: Unable to Locate Boot Info (Major)

Description

The system cannot locate the bootinfo file that should be present in the same directory as the RTC boot file.

This alarm is caused when the file is deleted or renamed.

Corrective action

To clear this alarm, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Network, 9: Unable to Locate Sysconf (Major)

Description

The system cannot locate the sysconf file that should be present in the same directory as the RTC load file.

This alarm is caused when the file is deleted or renamed.

Corrective action

To clear this alarm, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Network, 10: Unable to Parse Bootinfo (Major)

Description

The system was not able to parse the bootinfo file.

This alarm occurs when data in the bootinfo file becomes corrupted.

Corrective action

To clear this alarm, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Network, 11: Unable to Parse Sysconf (Major)

Description

The system was unable to parse the sysconf file.

This alarm occurs when data in the sysconf file becomes corrupted.

Corrective action

To clear this alarm, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Network, 12: Unable to Locate RTC Load (Major)

Description

The system could not locate the local directory or the RTC load on the alternate boot server.

This alarm has one of the following causes:

- The system could not locate the load directory indicated in the bootinfo file.
- The system could not locate the load file indicated in the sysconf file.
- The system could not locate the release directory. The directory was un-installed or deleted.
- The bootinfo file has become corrupted.

- The sysconf file has become corrupted.

Corrective action

Determine the possible cause of the alarm and perform the appropriate corrective action procedure as necessary.

If the release directory was deleted in error, re-install the release directory. To do this using the GUI, perform the following procedure.

Reinstalling the release directory

Step	Action
	At the OAMP workstation
1	Open the Alternate Boot Server window. To do this, click **Administration>file-manager**.
2	From the Alternate Boot Server partition, click **abs files**.
3	From the active rtc partition, click **Load** and then click on the load name to expand the list of files.
4	Click the file that you want to re-install on the system.
5	Click the left facing arrow to move and install the rtc partition load file onto the ABS.

—End—

Reset the alternate boot server configuration

If this alarm was not caused by a missing release directory, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Network, 13: Unable to Locate RTC Snapshot (Major)

Description

The system could not locate the snapshot directory on the alternate boot server.

This alarm can have one of the following causes:

- The system could not locate the snapshot directory in the bootinfo file.
- The snapshot file may have been deleted.
- Data in the bootinfo file may have become corrupted.

Corrective action

To clear this alarm, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Network, 14: Load May be Invalid (Major)

Description

The rtcboot load may have been corrupted.

This alarm occurs when the rtcboot file size does not match the file size of the rtcboot load file indicated in the sysconf file. This may be the result of an incomplete file transfer.

Corrective action

To clear this alarm, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Network, 15: Snapshot May be Invalid (Major)

Description

This alarm occurs when the snapshot directory has become corrupted or there is another error with the directory.

This alarm has one of the following possible causes:

- The system cannot locate the snapshot.des file.
- The bootinfo file may be corrupted and pointing to an invalid snapshot directory.
- The snapshot may have been partially deleted.

Corrective action

To clear this alarm, reset the alternate boot server configuration using the procedure "Resetting the alternate boot server configuration" (page 90).

Power Alarms

Power, 1: Status Change (Major)

Description

One of the two -48V power feeds has been lost for this system node.

If similar power status alarms are received for each system node (RTC, CC, or application) on a CAM shelf, it is likely that one of the power sources for the CAM shelf has been interrupted, due to a pulled or cut cable, or through the loss of the power source.

If this alarm is received for one system node, this is likely due to a blown fuse on the TM of the system node.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- Inspect the cables.
- the TM of the affected system node.

Inspecting the cables

Step	Action
	At the OAMP workstation
1	View the Alarms window. To do this, click **Fault>alarms** on the main menu and click **Realtime**. If you are receiving similar alarms for each system node, visually inspect the system to determine whether any cables are disconnected or damaged.
2	If any cables are disconnected or damaged, reconnect or them.
3	Determine if the power source to the system has been lost or interrupted and correct.
4	View the Alarms window again. If this alarm is still displayed, the TM of the affected system node, using the procedure "Replacing mission cards or TMs in system nodes" (page 176).

—End—

SCCP Management Alarms

SCCP Management: Local Subsystem (LSS) Alarm (Critical, Major, Minor)

Description

This alarm occurs when one or more Local Subsystem Instances (LSSI) have been activated in a Local Subsystem (LSS), but none have become allowed. The LSS remains in the prohibited state.

Corrective action

Since each LSSI is associated with an Application Server (AS), if an AS becomes inactive, the associated LSSI becomes suspended. In order to return an LSSI from a suspended state to an allowed state, you must make sure that one or more of the AS's Application Server Processes (ASP) are active. Perform the following procedure to return an LSSI to an allowed state.

Returning an LSSI to an allowed state

Step	Action
	At the OAMP workstation
1	Make sure the ASP paths are up. To do this, click **Network Mgmt** on the main menu, click **IPS7** on the Network Management window, and click **ASP Paths** on the IPS7 window.
2	The provisioned paths appear in the Application Server Process Path Records list, near the bottom of the window. Click a path from the list to view its status. If the path status is Up, go to step 4.
3	If the state of the path is Down, click **Up** to change the state of the path to "Up".
4	Check each path for the ASP.
5	Make sure at least one ASP is activated. Click **Network Mgmt** on the main menu, click **IPS7** on the Network Management window, and click **ASP** on the IPS7 window. Provisioned application server processes appear in the Application Server Process Records list at that bottom of the window.
6	The status of each ASP appears in the ASP Status box. Wait a few minutes to see if the ASP becomes activated. If the ASP becomes activated and the alarm clears, the procedure is complete. If the alarm does not clear, contact your next level of support.

—End—

SCCP Management, 25: RSS Alarm (Major)

Description

An alarm will be asserted against a remote subsystem (RSS) when a Subsystem Prohibited (SSP) message is received from the far end. It will be only one alarm more than one RSS failure.

LOG_MAJOR: At least one RSS is prohibited.

LOG_NONE: All RSSs are available.

Corrective action

Search from Alarm Status field on the RSS Record of the RSS GUI to find out which RSSs are prohibited.

Shelf Alarms

Shelf, 2: Fan Status (Major)

Description

A fault in a CAM shelf's fan unit has been detected. This means that two or more of the fans in the fan unit may have failed, which will result in increased temperature levels within the CAM shelf.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- "Viewing the Alarms window" (page 97)
- "Reseating the fan tray" (page 97)
- "Replacing the fan tray" (page 98)
- "Replacing mission cards or TMs in system nodes" (page 176)

Viewing the Alarms window

Step	Action
	At the OAMP workstation
1	View the Alarms window. To do this, click **Fault>alarm** on the main menu. Click **Realtime** to see current the alarms.
2	Determine why you are receiving this alarm. To do this, view the Information box and perform the remaining procedures in this section as necessary.

—End—

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Reseating the fan tray

Step	Action
	At the USP chassis
1	Ensure the fan tray is seated properly.

2 Locate the air grill on the front of the affected CAM shelf and, using a flat blade screwdriver, loosen the two screws on the air grill by turning counter-clockwise 3/4 turn.

3 Grasp the lower edge of the fan tray, placing your thumbs on the two spring-release latches.

4 Press the two latches inward and up, gently pulling the fan tray toward you.

5 Slide the fan tray back into the CAM shelf until seated properly. Two audible clicks can be heard when the fan tray is seated properly.

6 Position the air grill on the fan assembly.

7 Using a flat blade screwdriver, turn the two screws on the air grill clockwise 3/4 turn.

8 View the Alarms window by clicking **Fault>alarm** on the main menu. Click **Realtime** to see the current alarms.

If this alarm is still displayed, the fan tray, as described in the next procedure.

—End—

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Replacing the fan tray

Step	Action

At the USP chassis

1 Obtain a new fan tray.

2 Locate the air grill on the front of the affected CAM shelf.

3 Using a flat blade screwdriver, loosen the two screws on the air grill by turning counter-clockwise 3/4 turn.

4 Gently pull the air grill toward you to remove it.

5 Grasp the lower edge of the fan tray, placing your thumbs on the two spring-release latches. Press the two latches inward and up, gently pulling the fan tray toward you.

6 Lift the new fan tray and slide into the CAM shelf until seated properly. Two audible clicks can be heard when the fan tray is seated properly.

7 Position the air grill on the fan assembly.

8 Using a flat blade screwdriver, turn the two screws on the air grill clockwise 3/4 turn.

9 View the Alarms window by clicking **Fault>alarm** on the main menu. Click **Realtime** to see the current alarms.

10 If this alarm is still displayed, the TMs of the CC system nodes, as described in "Replacing mission cards or TMs in system nodes" (page 176).

—End—

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Shelf, 2: Fan Status (Minor)

Description

A fault has been detected in a CAM shelf's fan unit, indicating that one of the fans in the fan unit may have failed. This can result in increased temperature levels within the CAM shelf.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- Reseat the fan tray, see "Reseating the fan tray" (page 97).
- the fan tray, see "Replacing the fan tray" (page 98).
- the TMs of the CC system nodes, see "Replacing mission cards or TMs in system nodes" (page 176).

Shelf, 3: Temperature Fault (Major)

Description

This alarm occurs when a CAM shelf temperature exceeds the maximum operating temperature.

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- Check the ambient temperature, see "Checking the ambient temperature" (page 100).
- the air filter, see "Replacing the air filter" (page 100).
- Reseat the fan tray, see "Reseating the fan tray" (page 97).
- the fan tray, see "Replacing the fan tray" (page 98).
- the TMs of the CC system nodes, see "Replacing mission cards or TMs in system nodes" (page 176).

Checking the ambient temperature

Step	Action
	At the OAMP workstation
1	Ensure that the ambient temperature is set to an acceptable level in the room where the system is located. If it is not, determine the cause and correct it.
2	View the Alarms window by clicking **Fault>alarm** on the main menu. Click **Realtime** to see the current alarms.
3	On the Alarms window, determine why you are receiving this alarm by viewing the Information box and complete the following procedure(s), as necessary.

—End—

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Replacing the air filter

Step	Action
	At the USP chassis
1	Obtain a new air filter.
2	Locate the air grill on the front of the affected CAM shelf.

3 Using a flat blade screwdriver, loosen two screws on the face of the grill by turning counter-clockwise 3/4 turn.

4 Gently pull the air grill toward you to remove.

5 Locate the thumbscrew on the front of the fan assembly.

6 Rotate the thumbscrew counter clockwise to loosen.

7 Slide the metal plate, located behind the thumbscrew, left or right to release the air filter.

8 Pull the air filter toward you to remove.

9 Slide the new air filter into the air filter slot.

10 Apply pressure to the front of the air filter until it is flush with the fan assembly.

11 Slide the metal plate back to the center position.

12 Turn the thumbscrew clockwise to tighten.

13 Position the air grill on the fan assembly.

14 Using a flat blade screwdriver, turn the two screws on the air grill clockwise 3/4 turn.

ATTENTION
Following the instructions on the front of the air filter, the air filter may be washed, dried, and reused.

15 View the Alarms window by clicking **Fault>alarm** on the main menu. Click **Realtime** to see the current alarms.

16 If this alarm is still displayed, reseat the fan tray, as described in "Reseating the fan tray" (page 97).

17 If this alarm is still displayed, the fan tray, as described in "Replacing the fan tray" (page 98).

18 If this alarm is still displayed, the TMs of the CC system nodes, as described in "Replacing mission cards or TMs in system nodes" (page 176).

—End—

System Node Maintenance Alarms

System Node Maintenance, 3: Disable State Transition (Major)

Description

The operational state of a node became disabled. Refer to the User Guide for information about the operational states of the USP. System impact varies depending on the type of system node that is disabled.

Disabled Node Transition Alarm Impact

System Node	Components	Effect When Disabled
SS7 Link	SS7 Link mission card DS0A TM or V.35 TM	DS0A or V.35 ports associated with the Link system node are unavailable. SS7 traffic may be affected, depending on traffic configuration.
SS7 IP Link	SS7 IP Link mission card Power/SCS/ Ethernet (PSE) TM	Links associated with the SS7 IP Link system node are unavailable. IP traffic may be affected, depending on traffic configuration.
IP Link	IP Link mission card Power/SCSI/ Ethernet (PSE) TM	Paths associated with the IP Link system node are unavailable. IP traffic may be affected, depending on traffic configuration.

System Node	Components	Effect When Disabled
CC	CC mission card OC-3TM	If CC system nodes are disabled, internal switch communications and/or SS7/IP traffic may be affected. If one CC system node on a CAM shelf is disabled, a loss of redundancy occurs for internal CAM shelf communications and inter-shelf communication (in a dual-shelf system only). If both CC system nodes are disabled on either a control CAM shelf or an extension CAM shelf, a loss of internal communications occurs for the CAM shelf, and a dual-shelf system will go into isolation.
RTC	RTC mission card SCSI Disk card PSE TM Filler card	If one RTC is disabled, a loss of RTC redundancy occurs. If both RTCs are disabled, OAMP communications to the USP is lost, and SS7 dynamic management control is unavailable.
NPC	NP mission card SCSI Disk card PSE TMs	If Number Portability Controller (NPC) system nodes are disabled, NP query rates may be affected. If one NPC system node is disabled, the associated local subsystem (LSS) instance is suspended. If both NPC system nodes are disabled, the associated LSS instances are suspended, connection to the provisioning system is broken, and the ability to update the application database is lost.

System Node	Components	Effect When Disabled
NPS	NP mission card SCSI Disk card	If Number Portability Server (NPS) system nodes are disabled, application query rates may be affected.
	PSE TMs	If one NPS system node is disabled, the associated LSS instance is suspended. If more than one of the NPS system nodes are disabled, the associated LSS instances are suspended and your application subsystem could become congested.
NPE	NP mission card PSE TMs	If Number Portability Extension (NPE) system nodes are disabled, NP query rates may be affected. If one or more NPE cards in the same chain are disabled, the entire chain becomes disabled. The LSS instances associated with the chain continue to use the mate chain with no traffic impact. If more than one NPE is disabled in more than one chain, then multiple chains go down, and query processing could become congested depending on the number of LSS instances impacted.

This alarm is caused by the following:

- A system node (RTC, application, or CC) is loaded from the USP GUI.
- The USP is under going a complete office recovery (COR) operation.
- Application system node failures, which are caused by the following:
  - — a software exception
  - — loss of communication from CC system nodes to application system node
  - — dual CC system node failure
  - — a hardware failure

- CC system node failures, which are caused by the following:
  - loss of communications from the RTC system node(s) to CC system node
  - a software exception
  - a hardware failure
- RTC system node failures, which are caused by the following:
  - a software exception
  - a hardware failure

Corrective action

To clear this alarm, complete the following procedure(s), as necessary:

- Recover a CC system node, see "Recover a CC system node" (page 105).
- Recover an application system node, see "Recover an application system node" (page 106).
- Recover an RTC system node, see "Recover an RTC system node" (page 107).

Recover a CC system node

To recover a CC system node, complete the following procedure(s), as necessary.

- Load the CC system node, see "Loading a system node" (page 163).
- Reseat the card in the system node, see "Reseating cards in system nodes" (page 181).
- Replace the card in the system node, see "Replacing mission cards or TMs in system nodes" (page 176).

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Recovering a CC system node

Step	Action
	At the OAMP workstation
1	Perform the procedure "Loading a system node" (page 163).

2 As instructed in the loading procedure, if the CC system node does not return to full service, perform the procedure "Reseating cards in system nodes" (page 181) for the mission card and TM of the CC system node.

3 Perform the procedure "Replacing mission cards or TMs in system nodes" (page 176).

—End—

Recover an application system node

To recover an application system node, complete the following procedures:

- Enable a CC system node, see "Enabling a CC system node" (page 34).
- Load an application system node, see "Loading an application system node" (page 106).
- Reseat cards in system nodes, see "Reseating cards in system nodes" (page 35).
- Replace mission cards or TMs in system nodes, see "Replacing mission cards or TMs in system nodes" (page 176).
- Verify the operational mode of each V.35 port, see "Verify the Operational Mode of Each V.35 TM Port" (page 185).

Loading an application system node

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node**.
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click the icon for the affected system node. The Administration panel appears.
4	If the system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.
5	Click **Load**. Wait for the system node to enable and click **Unlock** (with confirmation) to ensure the system node returns to full service.
6	If the affected system node was an IP link system node, determine if all ASPs are back in service. If any ASPs are still out of service, activate the paths for each ASP. See the Configuration guide for more information.

7 If the system node does not return to full service, perform "Reseating cards in system nodes" (page 181) and repeat this procedure.

—End—

Recover an RTC system node

Before an RTC system node can be recovered, you must ensure at least one CC system node is enabled. To do this, complete the following procedure.

To recover a CC system node, complete the following procedure(s), as necessary.

- Load the CC system node, see "Loading a system node" (page 163).
- Reseat the card in the system node, see "Reseating cards in system nodes" (page 181).
- Replace the card in the system node, see "Replacing mission cards or TMs in system nodes" (page 176).

System Node Maintenance, 12: Locked Active RTC (Critical)

Description

This alarm indicates that a locked RTC system node has gained activity for the mate RTC system node.

Corrective action

Unlock one or both RTC system nodes by performing the following procedure.

Unlocking RTC system node

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node**.
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click the icon for the affected RTC system node. The associated provisioning and maintenance window appears.
4	Click **Unlock**. At the confirmation prompt, click **Yes**.
5	If necessary, repeat step 2 through step 4 to unlock the other RTC system node.

—End—

System Node Maintenance, 32: Dual CC Failure (Critical)

Description

Both CC system nodes failed on a control CAM shelf. This can be caused by the following:

- loss of communications from the RTC system nodes to the CC system nodes
- a software exception
- a hardware failure

Corrective action

Depending on the cause of this alarm, complete the following procedure(s) for each CC system node, as necessary:

- Load the CC system node, see "Loading the CC system node" (page 108).
- Reseat the mission cards and/or TMs, see "Reseating cards in system nodes" (page 35).
- Replace the mission cards and/or TMs, see "Replacing mission cards or TMs in system nodes" (page 176).

CAUTION
Do not make provisioning or maintenance changes on the system while this alarm is in effect, except those required to clear the alarm. Provisioning/maintenance changes may be lost as the system recovers from this alarm.

Loading the CC system node

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node**.
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click the icon for the affected system node. The Administration panel appears.
4	If the system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

5 Click **Load**. Wait for the system node to enable and click **Unlock** (with confirmation) to ensure the system node returns to full service.

6 If the CC system node does not return to full service, reseat the mission card and TM of the CC system node, as described in the procedure "Reseating cards in system nodes" (page 35).

—End—

System Node Maintenance, 38: Loss of Signal (Major)

Description

A CC system node can no longer detect a signal transmitting through its fiber-optic cable.

Loss of signal (LOS) is caused by one or a combination of the following factors:

- disconnection of the fiber-optic cable
- failure of the fiber-optic cable
- failure of one or both of the CC mission cards at either end of the cable
- failure of one or both of the OC-3 TM cards at either end of the cable

The alarm information identifies which path is affected, either the path between the CC system nodes in slot 1 of each shelf, or the path between the CC system nodes in slot 18 of each shelf. You should perform the corrective action for the affected path only, unless both paths have an LOS alarm. If both paths are reporting LOS alarms, you should perform the corrective procedures for one path at a time.

When a single LOS occurs, communication redundancy is lost. The fiber-optic cable remaining in operation, and the CC system nodes to which it is connected handle all communication between the control CAM shelf and the extension CAM shelf.

As a result, while it detects LOS, the system prohibits the following actions on the CC system nodes in the other path:

- locking
- loading
- offlining

Corrective action

To correct an LOS condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the LOS alarm clears before proceeding to the next set of instructions.

- Check the physical connections of the fiber-optic cable, see "Check the physical connections of the fiber-optic cable" (page 110).
- Replace the fiber-optic cable, see "Replacing the fiber-optic cable" (page 110).
- Reseat the mission card and TM of the extension CAM shelf CC system node, see "Reseating cards in system nodes" (page 35).
- Replace the mission card and TM of the extension CAM shelf CC system node, see "Replacing mission cards or TMs in system nodes" (page 176).
- Reseat the mission card and TM of the control CAM shelf CC system node, see "Reseating cards in system nodes" (page 35).
- Replace the mission card and TM of the control CAM shelf CC system node, see "Replacing mission cards or TMs in system nodes" (page 176).

Check the physical connections of the fiber-optic cable

To ensure the fiber-optic cable is connected properly, verify that both ends of the cable are plugged securely into the receptacles on the OC-3 TM cards at the rear of each CAM shelf.

Wait five minutes to see if the LOS alarm clears before proceeding to the next section.

Replacing the fiber-optic cable

Step	Action
	At the USP chassis
1	Remove the old cable. To do this, grasp the connector at the rear of the OC-3 TM of the CC system node in the extension CAM shelf and gently pull it toward you. Grasp the connector at the rear of the OC-3 TM of the CC system node of the control CAM shelf and gently pull it toward you.
2	Install the new cable. To do this, insert the connector at the end of the cable into the receptacle at the rear of the OC-3 TM in the CC system node of the control CAM shelf, ensuring that it is secure. Insert the other connector into the receptacle at the rear of the OC-3 TM in the CC system node, ensuring that it is secure.

3 Wait five minutes to see if the LOS alarm clears before proceeding to the next section.

—End—

System Node Maintenance, 40: Isolation (Critical)

Description

Both communication paths between the control CAM shelf and the extension CAM shelf have failed, resulting in the extension CAM shelf becoming isolated.

Isolation is caused by one or a combination of these factors:

- an offlined CC system node
- disabled CC system nodes
- loss of signal (LOS) conditions in one or both of the fiber-optic cables that connect the control CAM shelf and the extension CAM shelf

An extension CAM shelf is not considered isolated unless at least one CC system node is provisioned on it at the time that inter-shelf communication is disrupted.

During isolation, all the CC and application system nodes on the extension shelf will become disabled. When the isolation clears, the system will automatically attempt to restore all the CC and application system nodes that are not offline.

Because the extension CAM shelf CC and application system nodes are disabled during isolation, the system will prohibit most maintenance activities on them.

Prohibited maintenance activities include the following:

- locking or unlocking
- loading, except loading a disabled CC system node as part of isolation recovery
- running diagnostics
- switching activity (SWACT) of the active and inactive NPC system nodes
- setting or clearing loopback or BERT operations on a DS0A port or a V.35 port of a Link system node

Corrective action

To clear isolation, complete these procedure(s), in the following order. Wait five minutes after each procedure to see if the isolation conditions clears before proceeding with the next set of instructions.

- Ensure that the control CAM shelf CC system nodes are not offline, and recover if possible.
- Clear disabled alarms affecting the control CAM shelf CC system nodes.
- Clear the loss of signal (LOS) condition(s).
- Ensure that the extension CAM shelf CC system nodes are not offline, and recover if possible.
- Clear disabled alarms affecting the extension CAM shelf CC system nodes.

Recover offline control CAM shelf CC system modes

If a CC system node on the control CAM shelf is offline, the communication path between it and the corresponding extension CAM shelf CC system node will be unavailable. Check the availability status of the control CAM shelf CC system nodes. If one is offline, recover it:

Recovering control CAM shelf CC system nodes

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node**.
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click the icon for the intended CC system node. The Administration panel appears.

If the CC system node is:	Do:
offline	step 5 .
online	"Clear disabled alarms on control CAM shelf CC system nodes" (page 113).

4	If the CC system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

5 Click **Load** to download the boot image and re-initialize and enable the RTC system node. At the confirmation prompt, click **Yes**.

If the system node:	Do:
enabled	step 6.
did not enable	"Clear disabled alarms on control CAM shelf CC system nodes" (page 113).

6 After the CC system node loads, click **Unlock** (with confirmation) to ensure the system node returns to full service.

7 Repeat step 2 through step 6 for the second CC system node as necessary.

8 Wait five minutes to see if isolation clears before proceeding to "Clear disabled alarms on control CAM shelf CC system nodes" (page 113).

—End—

Clear disabled alarms on control CAM shelf CC system nodes

To clear disabled alarms on the control CAM shelf CC system nodes, perform the corrective actions for that alarm. See the procedure "Recovering a CC system node" (page 74).

Wait five minutes to see if isolation clears before proceeding to "Clear Loss of Signal (LOS) alarms" (page 113).

Clear Loss of Signal (LOS) alarms

To clear an LOS alarm, perform the corrective actions for that alarm. See "System Node Maintenance, 38: Loss of Signal (Major)" (page 109).

Wait five minutes to see if isolation clears before proceeding to the next section.

Recover offline extension CAM shelf system nodes

Check the availability status of the extension CAM shelf CC system nodes and recover them if they are offline.

Recovering offline extension CAM shelf system nodes

Step	Action
	At the OAMP workstation

1 Open the affected system shelf window. To do this, click **Configuration>platform>node**.

2 To view the CAM shelf icon, click **Graphical View**.

3 Double-click the icon for the intended CC system node. The Administration panel appears.

If the CC system node is:	Do:
offline	step 5.
online	"Clear disabled alarms on control CAM shelf CC system nodes" (page 113).

4 If the CC system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

5 Click **Load** to download the boot image and re-initialize and enable the RTC system node. At the confirmation prompt, click **Yes**.

If the system node:	Do:
enabled	step 6.
did not enable	"Clear disabled alarms on control CAM shelf CC system nodes" (page 113).

6 After the CC system node loads, click **Unlock** (with confirmation) to ensure the system node returns to full service.

7 Repeat step 2 through step 6 for the second CC system node as necessary.

8 Wait five minutes to see if isolation clears before proceeding to "Clear disabled alarms on control CAM shelf CC system nodes" (page 113).

—End—

Clear disabled alarms on extension CAM shelf CC system nodes

To clear disabled alarms on the extension CAM shelf CC system nodes, perform the corrective actions for that alarm. See the procedure "Clear disabled alarms on control CAM shelf CC system nodes" (page 113).

Wait five minutes to see if isolation clears before proceeding to the next section.

Contact your next level of support

If you complete all of these procedures and the isolation condition does not clear, contact your next level of support.

System Node Maintenance, 66: Node manually locked (Minor)

Description

The system generates this minor alarm when the user manually locks a node.

Correction action

To clear this alarm, the user must unlock the node manually.

Unlocking the system node manually

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node**.
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click the icon for the affected system node. The associated provisioning and maintenance window appears.
4	Click **Unlock**. At the confirmation prompt, click **Yes**.
5	If necessary, repeat step 2 through step 4 to unlock the other system nodes.

—End—

System Node Maintenance ICCM Alarms

System Node Maintenance, 40: Isolation (Critical)

Description

Both communication paths between the CAM Controllers (CC) on the control CAM shelf and the CCs on an extension CAM shelf have failed. Therefore, the extension CAM shelf is isolated.

Isolation is caused by one or a combination of these factors:

- an offlined CC system node
- disabled CC system nodes
- communication fault conditions in one or both of the fiber-optic cables that connect the CC and the termination point (either a CC on another shelf, or a line card on an ICCM)
- Inter-CAM Communication Medium (ICCM) failures

The alarm information identifies whether the problem is on the receive (RX) or transmit (TX) fiber-optic cable. The alarm indicates whether the CC affected is in slot 1 or slot 18, and indicates the shelf on which the CC resides. In this case, the alarm indicates a fault on the receive path of the CC. Perform the corrective action for this path only. If more than one CC reports an isolation fault, clear the alarms one at a time.

During isolation, all the CC and application system nodes on the isolated extension CAM shelf become disabled. When the isolation clears, the system normally attempts to restore all the CC and application system nodes that are not offline.

Because the CC and application system nodes for the shelf are disabled during isolation, the system prohibits most maintenance activities on them.

Prohibited maintenance activities include:

- locking or unlocking
- loading, except loading a disabled CC system node as part of isolation recovery
- running diagnostics
- switching activity (SWACT) of the active and inactive NPC system nodes
- setting or clearing loopback or BERT operations on a DS0A port or a V.35 port of a Link system node

Corrective action

To clear isolation, complete these procedure(s), in the following order. Wait five minutes after each procedure to see if the isolation condition clears before proceeding with the next set of instructions.

- Make sure that the control CAM shelf CC system nodes are not offline, and recover if possible.
- Clear disabled alarms affecting the control CAM shelf CC system nodes.
- Clear the communication fault(s).
- Make sure that the extension CAM shelf CC system nodes are not offline, and recover if possible.
- Clear disabled alarms affecting the extension CAM shelf CC system nodes.

Recover offline control CAM shelf CC system nodes

If a CC system node on the control CAM shelf is offline, the communication path between it and all extension CAM shelf CC system nodes (for dual-shelf systems) or ICCM (for multi-shelf systems) is not available.

To recover the affected CC on the control CAM shelf, perform the following procedure.

Recovering the affected CC system node on the control CAM shelf

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node.**
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click the icon for the intended CC system node. The Administration panel appears.

If the CC system node is:	Do:
online	"Clear disabled alarms on control CAM shelf CC system nodes" (page 118).
offline	step 4.

4	On the CC system node provisioning and maintenance window, click **Load**. The CC system node boot image is downloaded and the CC system node is re-initialized. If the CC system node becomes enabled, proceed to step 5. If it does not become enabled, stop this

procedure and skip "Clear disabled alarms on control CAM shelf CC system nodes" (page 118).

5 After the CC system node loads, click **Unlock**.

6 Repeat step 3 to step 5 for the remaining CC system node on the extension CAM shelf, if necessary.

Wait five minutes to see if isolation clears before proceeding to "Clear disabled alarms on control CAM shelf CC system nodes" (page 118).

—End—

Clear disabled alarms on control CAM shelf CC system nodes

To clear disabled alarms on control CAM shelf CC system nodes, perform the corrective actions for that alarm. See the procedures for recovering a CC system node in the System Node Maintenance, 3: Disable State Transition (Major) section of this manual.

Wait five minutes to see if isolation clears before proceeding to the next section.

Clear communication fault alarms

Clear any of the following communication fault alarms:

- Loss of Signal (LOS). To clear an LOS alarm, refer to System Node Maintenance, 38: Loss of Signal (Major).
- Loss of Frame (LOF). To clear an LOF alarm, refer to System Node Maintenance, 50: Loss of Frame (Major).
- Loss of Pointer (LOP). To clear an LOP alarm, refer to System Node Maintenance, 51: Loss of Pointer (Major).
- Loss of Cell Delineation (LCD). To clear an LCD alarm, refer to System Node Maintenance, 52: Loss of Cell Delineation (Major).

Wait five minutes to see if isolation clears before proceeding to the next section.

Recover offline extension CAM shelf system nodes

Refer to the log to determine the shelf and position of the CC. Recover any offline CCs. To do this, perform the procedure "Recovering the affected CC system node on the control CAM shelf" (page 117).

Contact your next level of support

If you complete all of these procedures and the isolation condition does not clear, contact your next level of support.

System Node Maintenance, 38: Loss of Signal (Major)

Description

A CC system node can no longer detect a signal on its receive (RX) fiber-optic cable segment.

Loss of signal (LOS) can be caused by one or a combination of the following factors:

- disconnection of the fiber-optic cable
- failure of the fiber-optic cable
- failure of the CC mission card
- failure of the OC-3 TM card
- failure of an ICCM

The system raises the alarm against the CC system node that detects the fault on its RX fiber-optic cable. The log information indicates the position and shelf of the CC system node. Because the alarm indicates the fault on the far end of the CC system node, perform corrective actions on the node at the far end, rather than the CC system node with the alarm. Perform the corrective action for this path only. If more than one CC reports an LOS fault, clear the alarms one at a time.

When a single LOS occurs, communication redundancy is lost for the shelf specified in the log information. The fiber-optic cable on the remaining plane, and the CC system node and far-end node (CC system node or ICCM) it connects, handle all communication for that shelf.

As a result, while it detects LOS, the system prohibits the following actions on the CC system nodes in the other path:

- locking
- loading
- offlining

Corrective action

To correct an LOS condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the LOS alarm clears before proceeding to the next set of instructions.

- Check the physical connections of the fiber-optic cable, see "Check the physical connections of the fiber-optic cable" (page 120).
- Replace the fiber-optic cable, see "Replacing the fiber optic cable (NTST20AA)" (page 120).
- Reseat the mission card and TM of the CAM shelf CC system node at the remote end, see "Reseating the mission card and TM of the CAM shelf CC system node" (page 121).

- Replace the mission card and TM of the CAM shelf CC system node at the remote end, see "Replacing the mission card and TM of the CAM shelf CC system node" (page 122).
- Check the ICCM alarms and logs for any problems, see "Check the ICCM" (page 124).

Check the physical connections of the fiber-optic cable

To make sure the fiber-optic cable is connected properly, make sure that both ends of the cable are plugged securely into the receptacles on the OC-3 TM card at the rear of the CAM shelf and the node at the remote end of the fiber-optic cable (a line card on the ICCM or a CC system node on another shelf).

Wait five minutes to see if the LOS alarm clears before proceeding to the next section.

CAUTION
Make sure that you pull the correct OC-3 cable for the CC and line card associated with the alarm. Pulling the wrong OC-3 cable can cause service disruption.

Replacing the fiber optic cable (NTST20AA)

Step	Action
	At the OAMP workstation
1	Remove the old cable. To do this, grasp the connector at the rear of the OC-3 TM of the CC system node in the CAM shelf and gently pull it toward you. Grasp the connector at the remote end and gently pull it toward you.
2	Install the new cable. To do this, insert the connector at the end of the cable into the receptacle at the rear of the OC-3 TM in the CC system node of the CAM shelf, making sure that it is secure. Insert the other connector into the receptacle at the remote end of the fiber-optic cable, making sure that it is secure.
3	Wait five minutes to see if the LOS alarm clears before proceeding to the next section.

—End—

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Reseating the mission card and TM of the CAM shelf CC system node

Step	Action

At the OAMP workstation

1 Attempt to lock and offline the CAM shelf CC system node. To do this, perform these steps:

If you are unable to lock and offline the CC system node, you can still proceed to step 2.

a. Open the affected system shelf window. To do this, click **Configuration>platform>node**.

b. To view the CAM shelf icon, click **Graphical View**.

c. Double-click the icon for the intended CC system node you are attempting to lock and offline. The Administration panel appears.

d. Click **Lock**. At the confirmation prompt, click **Yes**. If the CC system node locks, proceed to step step e. If it does not lock, skip to step 2.

e. Click **Offline**. At the confirmation prompt, click **Yes**. Proceed to step 2.

2 Before you reseat a CC mission card, unseat its corresponding OC-3 TM. Two audible clicks can be heard when the mission card or TM is released completely. Use the following procedure to unseat and reseat the OC-3 TM or CC mission card:

a. Press outward on the top and bottom latches of the mission card to release it from the CAM shelf.

b. Grasp the top and bottom latches of the mission card and gently pull it toward you to remove it from the CAM shelf.

c. Make sure the top and bottom latches are in the outward position by pressing outward on each latch.

d. Position the top and bottom latches facing you, and gently slide the mission card into the card guide of the one you removed, seating the bottom of the mission card into the card guide and then the top.

e. Apply pressure to the faceplate near the latches until you feel resistance.

f. Snap the top and bottom latches of the mission card inward, toward one another. Two audible clicks can be heard when the mission card is seated properly.

g. Repeat step a through step f to reseat the CC mission card.

3 On the front and rear of the CAM shelf, press Lamp Test. If the LEDs do not light for the CC system node, stop this procedure and skip to the procedure "Replacing the mission card and TM of the CAM shelf CC system node" (page 122). If the LEDs light, proceed to step 4.

4 On the CC system node provisioning and maintenance window, click **Load** and wait for the system node to enable.

5 Click **Unlock** to ensure the system node returns to full service.

6 Wait five minutes to see if the LOS alarm clears. If not, proceed to "Replacing the mission card and TM of the CAM shelf CC system node" (page 122).

—End—

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Replacing the mission card and TM of the CAM shelf CC system node

Step	Action

At the OAMP workstation

1 If the system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

ATTENTION
If the extension CAM shelf is in isolation, you cannot lock the CC system node. If this is the case, proceed to step 3.

2 Click **Offline**. At the confirmation prompt, click **Yes**.

ATTENTION
If the extension CAM shelf is in isolation and the CC system node is enabled, you cannot offline the CC system node. The CC system node must be offline in order to edit the card configuration.

3 Obtain a new mission card and TM, verify they have the correct PEC labels, and make sure the top and bottom latches are in the outward position.

ATTENTION

If the new mission card and TM have different PECs than the ones you are replacing, you must change the PEC in the Provisioning and Maintenance window before loading the card.

4 Before you replace a CC mission card, unseat and disconnect its corresponding OC-3 TM, removing the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors for the TM. Use the following procedure to unseat and replace the OC-3 TM or CC system node:

a. Press outward on the top and bottom latches of the mission card to release it from the CAM shelf. Two audible clicks can be heard when the mission card or TM is released completely.

b. Grasp the top and bottom latches of the mission card and gently pull it toward you to remove it from the CAM shelf.

c. On the new card, make sure the top and bottom latches are in the outward position by pressing outward on each latch.

d. Position the top and bottom latches facing you, and gently slide the mission card into the card guide of the one you removed, seating the bottom of the mission card into the card guide and then the top.

e. Apply pressure to the faceplate near the latches until you feel resistance.

f. Snap the top and bottom latches of the mission card inward, toward one another. Two audible clicks can be heard when the mission card is seated properly.

g. Repeat step a through step f to replace the CC system node.

5 After you reseat the OC-3 TM and CC system node, plug in the connectors and turn the thumbscrews on the top and bottom of the connectors to tighten.

6 On the front and rear of the CAM shelf, press Lamp Test. If the LEDs do not light for the system node you just replaced, make sure the mission card and TM are seated properly by unseating each and completing step 4 and step 5.

7 If the LEDs light, on the CC system node provisioning and maintenance window, click **Load** and wait for the system node to enable.

8 Click **Unlock** to ensure the system node returns to full service.

9 If the CC system node becomes enabled, wait five minutes to see if the LOS alarm clears. If the alarm does not clear, proceed to "Check the ICCM" (page 124). If the CC system node does not become enabled, contact your next level of support.

—End—

Check the ICCM

Check the ICCM for faults. For more information about the ICCM, refer to the document *Marconi TNX-210 ATM Switch User Manual*, available on the software or documentation CD-ROM. If you are not able to clear the alarm, contact your next level of support.

System Node Maintenance, 50: Loss of Frame (Major)

Description

A CAM Controller (CC) system node can no longer detect a SONET frame on its receive (RX) OC-3 cable that connects it to an Inter-CAM Communication Medium (ICCM) or a CC on another shelf.

Loss of Frame (LOF) can be caused by one or a combination of the following factors:

- failure of the ICCM
- failure of the OC-3 TM card

The system raises the alarm against the CC system node that detects the fault on its RX fiber-optic cable. The log information indicates the position and shelf of the CC system node. Because the alarm indicates the fault on the far end of the CC system node, perform corrective actions on the node at the far end, rather than the CC system node with the alarm. The alarm indicates whether the CC affected is in slot 1 or slot 18, and indicates the shelf on which the CC resides.

When a single LOF occurs, communication redundancy is lost for the remaining plane. The fiber-optic cable remaining in operation, and the CC system node and remote node (either a line card on an ICCM or a CC on another shelf) it connects, handle all communication for that shelf.

As a result, while it detects LOF, the system prohibits the following actions on the other CC system node on the shelf:

- locking

- loading
- offlining

Corrective action

To correct an LOF condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the LOF alarm clears before proceeding to the next set of instructions.

- Check the ICCM, see "Check the ICCM" (page 124).
- Reseat the mission card and TM of the CAM shelf CC system node at the remote end, see "Reseating the mission card and TM of the CAM shelf CC system node" (page 121).
- Replace the mission card and TM of the CAM shelf CC system node at the remote end, see "Replacing the mission card and TM of the CAM shelf CC system node" (page 122).

System Node Maintenance, 51: Loss of Pointer (Major)

Description

A CAM Controller (CC) system node can no longer detect a SONET pointer in the signal received through the OC-3 cable that connects it to the Inter-CAM Communication Medium (ICCM) or far-end CC.

Loss of Pointer (LOP) is caused by one or a combination of the following factors:

- failure of the ICCM
- failure of the CC mission card at the far end
- failure of the OC-3 TM card at the far end

The system raises the alarm against the CC system node that detects the fault on its RX fiber-optic cable. The log information indicates the position and shelf of the CC system node. Because the alarm indicates the fault on the far end of the CC system node, perform corrective actions on the node at the far end, rather than the CC system node with the alarm. The alarm indicates whether the CC affected is in slot 1 or slot 18, and indicates the shelf on which the CC resides.

When a single LOP occurs, communication redundancy is lost for the shelf specified in the log information. The fiber-optic cable remaining in operation, and the CC system node and ICCM or CC it connects, handle all communication for that shelf.

As a result, while it detects LOP, the system prohibits the following actions on the other CC system node on the shelf:

- locking

- loading
- offlining

Corrective action

To correct an LOF condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the LOF alarm clears before proceeding to the next set of instructions.

- Check the ICCM, see "Check the ICCM" (page 124).
- Reseat the mission card and TM of the CAM shelf CC system node at the remote end, see "Reseating the mission card and TM of the CAM shelf CC system node" (page 121).
- Replace the mission card and TM of the CAM shelf CC system node at the remote end, see "Replacing the mission card and TM of the CAM shelf CC system node" (page 122).

System Node Maintenance, 52: Loss of Cell Delineation (Major)

Description

A CAM Controller (CC) system node can no longer detect cell

delineation in the signal received through the OC-3 cable that

connects it to the Inter-CAM Communication Medium (ICCM) or CC at the far end.

Loss of Cell Delineation (LCD) is caused by one or a combination of the following factors:

- failure of the ICCM
- failure of the CC mission card
- failure of the OC-3 TM card

The system raises the alarm against the CC system node that detects the fault on its RX fiber-optic cable. The log information indicates the position and shelf of the CC system node. Because the alarm indicates the fault on the far end of the CC system node, perform corrective actions on the node at the far end, rather than the CC system node with the alarm. The alarm indicates whether the CC affected is in slot 1 or slot 18, and indicates the shelf on which the CC resides.

When a single LCD occurs, communication redundancy is lost for the shelf specified in the log information. The fiber-optic cable remaining in operation, and the CC system node and ICCM or CC it connects, handle all communication for that shelf.

As a result, while it detects LCD, the system prohibits the following actions on the other CC system node on the shelf:

- locking
- loading
- offlining

Corrective action

To correct an LCD condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the LCD alarm clears before proceeding to the next set of instructions.

- Check the ICCM, see "Check the ICCM" (page 124).
- Reseat the mission card and TM of the CAM shelf CC system node at the far end, see "Reseating the mission card and TM of the CAM shelf CC system node" (page 121).
- Replace the mission card and TM of the CAM shelf CC system node at the far end, see "Replacing the mission card and TM of the CAM shelf CC system node" (page 122).

System Node Maintenance, 53: Path Label Mismatch (Major)

Description

A CAM Controller (CC) system node detects a difference between the contents of the data package and the label for the package in the signal received through the OC-3 cable that connects it to the Inter-CAM Communication Medium (ICCM) or CC on the far end.

Path Label Mismatch (PLM) is caused by one or a combination of the following factors:

- failure of the ICCM
- failure of the CC mission card
- failure of the OC-3 TM card

The system raises the alarm against the CC system node that detects the fault on its RX fiber-optic cable. The log information indicates the position and shelf of the CC system node. Because the alarm indicates the fault on the far end of the CC system node, perform corrective actions on the node at the far end, rather than the CC system node with the alarm. The alarm indicates whether the CC affected is in slot 1 or slot 18, and indicates the shelf on which the CC resides.

When a single PLM occurs, communication redundancy is lost for the shelf specified in the log information. The fiber-optic cable remaining in operation, and the CC system node and ICCM or CC it connects, handle all communication for that shelf.

As a result, while it detects PLM, the system prohibits the following actions on the other CC system node on the shelf:

- locking
- loading
- offlining

Corrective action

To correct an PLM condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the PLM alarm clears before proceeding to the next set of instructions.

- Check the ICCM, see "Check the ICCM" (page 124).
- Reseat the mission card and TM of the CAM shelf CC system node at the far end, see "Reseating the mission card and TM of the CAM shelf CC system node" (page 121).
- Replace the mission card and TM of the CAM shelf CC system node at the far end, see "Replacing the mission card and TM of the CAM shelf CC system node" (page 122).

System Node Management, 59: Cable Fault

Description

The system detects a transmit (TX) fault on the OC-3 cable that connects a CAM Controller (CC) on a CAM shelf to a link card on an Inter-CAM Communication Medium (ICCM).

A Cable Fault alarm is caused by one or a combination of the following factors:

- disconnection of the OC-3 fiber optic cable
- failure of the OC-3 fiber optic cable
- communication failure, including LOS, LOF, LOP, LCD or PLM

The system raises the alarm against the CC system node that detects the fault on its TX fiber-optic cable. The log information indicates the position and shelf of the CC system node. The alarm indicates whether the CC affected is in slot 1 or slot 18, and indicates the shelf on which the CC resides.

When a single cable fault occurs, communication redundancy is lost for the shelf specified in the log information. The fiber-optic cable on the remaining plane, and the CC system node and ICCM or CC it connects, handle all communication for that shelf.

As a result, while it detects a cable fault, the system prohibits the following actions on the other CC system node on the shelf:

- locking
- loading
- offlining

Corrective action

To correct a cable fault condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the PLM alarm clears before proceeding to the next set of instructions.

- Check the physical connections of the fiber-optic cable, see "Check the physical connections of the fiber-optic cable" (page 129)
- Replace the fiber-optic cable, see "Replacing the fiber-optic cable (NTST20AA)" (page 129).
- Check the ICCM, see "Check the ICCM" (page 130).
- Check alarms for other communication faults, see "Check alarms for other communication faults" (page 130).

Check the physical connections of the fiber-optic cable

To make sure the fiber-optic cable is connected properly, make sure that both ends of the cable are plugged securely into the receptacles on the OC-3 TM cards at the rear of the CAM shelf and the line card on the ICCM.

Wait five minutes to see if the cable fault alarm clears before proceeding to the next section.

CAUTION
Make sure that you pull the correct OC-3 cable for the CC and line card associated with the alarm. Pulling the wrong OC-3 cable can cause service disruption.

Replacing the fiber-optic cable (NTST20AA)

Step	Action
	At the OAMP workstation
1	Remove the old cable. To do this, grasp the connector at the rear of the OC-3 TM of the CC system node in the CAM shelf and gently pull it toward you. Grasp the connector at the remote end and gently pull it toward you.
2	Install the new cable. To do this, insert the connector at the end of the cable into the receptacle at the rear of the OC-3 TM in the CC

system node of the CAM shelf, making sure that it is secure. Insert the other connector into the receptacle at the remote end of the fiber-optic cable, making sure that it is secure.

3 Wait five minutes to see if the LOS alarm clears before proceeding to "Check the ICCM" (page 130).

—End—

Check the ICCM

Check the ICCM for faults. For more information about the ICCM, refer to the document *Marconi TNX-210 ATM Switch User Manual*, available on the USP software or documentation CD-ROM. If you are not able to clear the alarm, contact your next level of support.

Check alarms for other communication faults

Check the alarms and logs for other communication faults, such as LOS, LOF, LOP, LCD, and PLM, that may exist on the CC system node. For information about clearing these alarms, refer to the sections System Node Maintenance, 38: Loss of Signal (Major), System Node Maintenance, 50: Loss of Frame (Major), System Node Maintenance, 51: Loss of Pointer (Major), System Node Maintenance, 52: Loss of Cell Delineation (Major), or System Node Maintenance, 53: Path Label Mismatch (Major).

System Node Management, 60: Remote Failure Indication (Major)

Description

The system detects a transmit (TX) fault on the OC-3 cable between the CAM Controller (CC) system node and the link card of the Inter-CAM Communication Medium (ICCM). The exact nature of the fault is not identified.

Remote Defect Indication (RDI) is caused by one or a combination of the following factors:

- disconnection of the OC-3 fiber optic cable
- failure of the OC-3 fiber optic cable
- failure of the CC mission card
- failure of the OC-3 TM card
- failure of the ICCM
- communication failure (LOS, LOF, LOP, LCD or PLM)

The system raises the alarm against the CC system node that detects the fault on its TX fiber-optic cable. The alarm indicates whether the CC affected is in slot 1 or slot 18, and indicates the shelf on which the CC resides.

When a single RDI occurs, communication redundancy is lost for the shelf specified in the log information. The fiber-optic cable on the remaining plane, and the CC system node and ICCM or CC it connects, handle all communication for the shelf.

As a result, while it detects RDI, the system prohibits the following actions on the other CC system node on the shelf:

- locking
- loading
- offlining

Corrective action

To correct an RDI condition, perform these procedures in the following order. Wait at least five minutes after each procedure to see if the RDI alarm clears before proceeding to the next set of instructions.

- Check the physical connections of the fiber-optic cable, see "Check the physical connections of the fiber-optic cable" (page 131).
- Replace the fiber-optic cable, see "Replacing the fiber-optic cable (NTST20AA)" (page 129).
- Reseat the mission card and TM of the CAM shelf CC system node, see "Reseating the mission card and TM of the CAM shelf CC system node" (page 121).
- Replace the mission card and TM of the CAM shelf CC system node, see "Replacing the mission card and TM of the CAM shelf CC system node" (page 122).
- Check the ICCM, see "Check the ICCM" (page 130).
- Check alarms for other communication faults, see "Check alarms for other communication faults" (page 131).

Check the physical connections of the fiber-optic cable

To make sure the fiber-optic cable is connected properly, make sure that both ends of the cable are plugged securely into the receptacles on the OC-3 TM cards at the rear of the CAM shelf and the line card on the ICCM.

Wait five minutes to see if the cable fault alarm clears before proceeding to "Check alarms for other communication faults" (page 131).

Check alarms for other communication faults

Check the alarms and logs for other communication faults, such as LOS, LOF, LOP, LCD, and PLM, that may exist on the CC system node. For information about clearing these alarms, refer to the sections System Node Maintenance, 38: Loss of Signal (Major), System Node Maintenance, 50:

Loss of Frame (Major), System Node Maintenance, 51: Loss of Pointer (Major), System Node Maintenance, 52: Loss of Cell Delineation (Major), or System Node Maintenance, 53: Path Label Mismatch (Major).

Task Management Alarms

Task Management, 9: Idle Task Starvation Threshold Reached

Description

The system generates this alarm when the idle task duration OM crosses the defined threshold value. This means that the applicable system node is running low on system resources.

Corrective action

Contact your next level of support.

Time of Day Alarms

Time of Day, 3: Timeout While Waiting for SNTP Server Reply (Minor)

Description

The system generates this alarm when the simple network time protocol (SNTP) client times out while waiting for a reply from the server.

Corrective action

Change the IP address of the SNTP to that of a working SNTP server. When the system receives a response from a working server, the system clears the alarm. Perform the following procedure.

Changing the IP address of the SNTP server

Step	Action
	At the OAMP workstation
1	Click **Administration>date-time**.
2	Add a new IP address for a different SNTP server in the **sntp-server** field.
3	Click **Modify** to submit the changes.
4	Click **Yes** at the confirmation prompt.
5	If the system does not automatically clear the alarm with the new SNTP server, contact your next level of support.

—End—

Time of Day, 4: Problem with Received SNTP Packet (Minor)

Description

The system generates this alarm when the simple network time protocol (SNTP) client receives invalid data from the SNTP server.

Corrective action

Change the IP address of the SNTP to that of a working SNTP server. When the system receives a response from a working server, the system clears the alarm. Perform the procedure "Changing the IP address of the SNTP server" (page 134).

GUI Error Messages

This section identifies the most common error messages displayed the GUI. With each message, diagnostic procedures or additional information are provided.

The GUI lost communication with the active RTC system node at IP xx.xx.xx.xx.

Description

Connectivity may have been lost on a device on your LAN.

This condition can be caused by the following:

- Cables to the specified device are improperly connected or damaged.
- The IP address of the specified device is incorrect.
- The specified device is powered off or is faulty.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: The GUI lost communication with the active RTC system node at IP xx.xx.xx.xx.

Step	Action
	At the OAMP workstation
1	Exit the GUI.
2	Attempt to log in again.
3	If you cannot log in, refer to the Local Device Fail procedure.

—End—

The GUI has lost communication with the inactive RTC system node at IP xx.xx.xx.xx.

Description

Connectivity may have been lost on a device on your LAN.

This condition can be caused by the following:

- Cables to the specified device are improperly connected or damaged.
- The IP address of the specified device is incorrect.
- The specified device is powered off or is faulty.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: The GUI lost communication with the inactive RTC system node at IP xx.xx.xx.xx.

Step	Action
	At the OAMP workstation
1	Exit the GUI.
2	Attempt to log in again.
3	If you cannot log in, refer to the Local Device Fail procedure.

—End—

This GUI session will terminate because it is not communicating with the tasks on the RTC system node.

Description

This message always follows a message that indicates a loss of communication with a Real-time Controller (RTC) system node.

This condition can be caused by the following:

- Cables to the specified device are improperly connected or damaged.
- The IP address of the specified device is incorrect.
- The specified device is powered off or is faulty.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: This GUI session will terminate because it is not communicating with the tasks on the RTC system node.

Step	Action
	At the OAMP workstation
1	Exit the GUI.
2	Attempt to log in again.
3	If you cannot log in, refer to the Local Device Fail procedure.

—End—

The maximum number (2) of GUI sessions are connected. Close one connection and try again.

Description

This message is for information purposes only.

Corrective action

Perform the following procedure.

Closing a GUI connection

Step	Action
	At the OAMP workstation
1	Close one existing GUI session.
2	Try to connect the new GUI session.
	—End—

A connection to xxxxx already exists. You may reset to remove the existing connection and begin a new one. Do you want to reset the connection?

Description

A connection already exists.

Corrective action

To clear this alarm, perform the following procedure.

Resetting a GUI connection

Step	Action
	At the OAMP workstation
1	Press Ctrl+Alt+Delete to determine if there are any tasks running with <not responding> after it.
2	Check the taskbar for minimized or hidden GUI connections.
3	If the task is hung, respond Y (yes) to reset the connection.
	—End—

Timeout waiting for a response from the RTC system node.

Description

This message indicates that the RTC system node has failed to respond to a request. This may or may not be a result of a user action.

The caption at the top of the window shows the request to which the RTC system node did not respond.

Corrective action

No corrective action is required. Click OK and proceed as normal.

A dual CC system node failure has occurred. The GUI is connecting to the RTC system node at IP xx.xx.xx.xx.

Description

Your system is in a dual Communications Applications Module (CAM) Controller (CC) system node failure condition. The GUI assumes that the RTC system node in slot 12 (RTC12) (if available) is active. Do not provision until this problem is corrected.

Connectivity may have been lost on a device on your LAN.

This condition can be caused by the following:

- Cables to the specified device are improperly connected or damaged.
- The IP address of the specified device is incorrect
- The specified device is powered off or is faulty.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: A dual CC system node failure has occurred. The GUI is connecting to the RTC system node at IP xx.xx.xx.xx.

Step	Action
	At the OAMP workstation
1	Exit the GUI.
2	Attempt to log in again.
3	If you cannot log in, refer to the Local Device Fail procedure.

—End—

The GUI failed to connect to the RTC system node at IP xx.xx.xx.xx.

Description

Connectivity may have been lost on a device on your LAN.

This condition can be caused by the following:

- Cables to the specified device are improperly connected or damaged.
- The IP address of the specified device is incorrect.
- The specified device is powered off or is faulty.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: The GUI failed to connect to the RTC system node at IP xx.xx.xx.xx.

Step	Action
	At the OAMP workstation
1	Exit the GUI.
2	Attempt to log in again.
3	If you cannot log in, refer to the Local Device Fail procedure.
	—End—

Out of stack space error. This may indicate an OAMP workstation problem.

Description

This message indicates a possible OAMP workstation problem.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: Out of stack space error. This may indicate an OAMP workstation problem.

Step	Action
	At the OAMP workstation
1	Close some of the applications that are open on the OAMP workstation.
2	Check the OAMP workstation memory.

3 Reboot the OAMP workstation.

4 If the problem continues, refer to the OAMP workstation is not Functioning Properly procedure.

5 Contact your next level of support.

—End—

Out of memory error. This may indicate an OAMP workstation problem.

Description

This message indicates a possible OAMP workstation problem.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: Out of memory error. This may indicate an OAMP workstation problem.

Step	Action
	At the OAMP workstation
1	Close some of the applications that are open on the OAMP workstation.
2	Check the OAMP workstation memory.
3	Reboot the OAMP workstation.
4	If the problem continues, refer to the OAMP workstation is not Functioning Properly procedure.
5	Contact your next level of support.

—End—

Unknown error *error number* received. Module: *module name*.

Description

An internal error has occurred.

Corrective action

Note the error number and module name and contact your next level of support.

File transfer failed. Please try again.

Description

The attempt to transfer a file from the RTC system node failed.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: File transfer failed. Please try again.

Step	Action
	At the OAMP workstation
1	If this error occurred while opening a window and no data is displayed in the window, close and reopen the window.
2	If the error recurs, contact your next level of support.

—End—

Warning: The GUI cannot communicate with the mate RTC system node. If you try to switch activity (SWACT), this GUI session will terminate. SWACT slotname?

Description

The inactive RTC system node is enabled, but the GUI does not have a connection to it.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: Warning: The GUI cannot communicate with the mate RTC system node. If you try to switch activity (SWACT), this GUI session will terminate. SWACT slotname?

Step	Action
	At the OAMP workstation
1	To determine why the GUI is not connected to the inactive RTC system node, refer to the Local Device Fail procedure.
2	Log off the GUI.
3	Log in to the GUI.

—End—

As an alternate approach, you can perform a SWACT. If you do this, the GUI will terminate the session. You will need to log back in to see if the SWACT completed successfully.

Unable to login. The file ss7db.mdb is locked by another task. Error: 75: Path/File access error

Description

A database needed for login is locked by a previous connection.

Corrective action

To clear this alarm, perform the following procedure.

Clearing: Unable to login. The file ss7db.mdb is locked by another task. Error: 75: Path/File access error.

Step	Action
	At the OAMP workstation
1	Press Ctrl+Alt+Delete to open the Close Program window.
2	Click SSGHMI <not responding>.
3	Click **End Task**.
4	Attempt to log in again.

—End—

Faults: Correcting OAMP Workstation/Networking Errors

This section identifies OAMP (operations, administration, maintenance, and provisioning) workstation and networking problems which you might encounter and provides basic troubleshooting procedures to help solve those problems.

Troubleshooting procedures are provided for the following:

- display problems
- OAMP workstation is not functioning properly
- GUI is not functioning properly
- OAMP workstation disk is full
- LAN-to-LAN/dial-up connection fails
- local device failures

Display problems

Description

The main menu is not centered on your desktop or is not visible on your desktop after you log in.

Corrective action

To solve the problem with the display, perform the following procedure.

Troubleshooting display problems

Step	Action
	At the OAMP workstation
1	Open the Display Properties window. To do this, click **Start**, select **Settings**, and then **Control Panel**.
2	On the Display Properties window, click **Settings** and ensure that the following display settings are set: • desktop area = 1024x768 • color palette = 16-bit (minimum) • font size = Small Fonts
3	Click **OK**.

—End—

OAMP workstation is not functioning properly

Description

These procedures will help you determine why your OAMP workstation is not functioning properly and give you the basic steps to correct the problem.

Corrective action

If the monitor on your OAMP workstation is not functioning or your workstation will not boot, perform the following procedure.

Troubleshooting workstation problems

Step	Action
	At the OAMP workstation
1	Ensure that the workstation and monitor are turned on (power light should be illuminated).
2	Check the workstation contrast and brightness settings.
3	Verify that all cables and power cords are plugged in.
4	Ensure that the power outlet is working. If the monitor on your OAMP workstation is still not functioning, contact your next level of support.

—End—

GUI is not Functioning Properly

Description

This section provides information to help you determine why your system's GUI is not functioning properly and gives you the procedure to correct the problem.

Corrective action

Corrective actions vary according to the particular situation. The following sections list several possible situations and their appropriate actions.

GUI is not running

If you try to access the GUI and it does not respond, contact your next level of support.

GUI is hung or is not responding

If the GUI is active but it is hung or not responding, you must restart your OAMP workstation.

Restarting your OAMP workstation

Step	Action
	At the OAMP workstation
1	Simultaneously press Ctrl+Alt+Delete on your keyboard.
	ATTENTION If your workstation does not respond after pressing Ctrl+Alt+Delete, you must power down the workstation.
2	On the Close Program window, highlight SSGHMI and click **End Task**. This exits the GUI.
3	If the message "Task not responding" appears, click **End Task** again.
4	From the task bar, click **Distinct NFS Server**. The Distinct NFS Server window appears.
5	From the Configure menu, select **Administrator** and then **Login**. The Administrator Login window appears.
6	Enter the password for your NFS Server in the System Administrator Password box and click **OK**.
7	From the Distinct NFS Server window, click the **Configure** menu again and select **Exit**. If your workstation is not set up as an alternate boot server, click **Start**, select **Shut Down**, select **Restart the Computer**, and then click **Yes**. If your workstation is set up as an alternate boot server, continue with step 8.
8	From the task bar, click **Distinct BOOTP Server**. The Distinct BOOTP Server window appears.
9	From the Configure menu, select **Administrator** and then **Login**. The Administrator Login window appears.
10	Enter the user-assigned password for the BOOTP Server in the System Administrator Password box and click **OK**.
11	From the Distinct BOOTP Server window, click the **Configure** menu again and select **Exit**.

12 From the task bar, click **Distinct FTP Server**. The Distinct FTP Server window appears.

13 From the **Configure** menu, select **Administrator** and then **Login**. The Administrator Login window appears.

14 Enter the user-assigned password for the FTP Server in the System Administrator Password box and click **OK**.

15 From the Distinct FTP Server window, click the **Configure** menu again and select **Exit**.

16 Click **Start**, select **Shut Down**, select **Restart the Computer**, and then click **Yes**.

—End—

GUI terminates abnormally

If the GUI terminates abnormally, the following messages may appear:

- runtime errors
- general protection faults

Runtime errors

If you receive a runtime error, perform the following procedure.

Troubleshooting runtime errors

Step	Action
	At the OAMP workstation
1	On the Runtime Error window, click **Details**, noting the details about why this error occurred.
2	Simultaneously press Ctrl+Alt+Delete on your keyboard. The Close Program window appears. Note the programs that were active and exit all running programs.
3	Restart your OAMP workstation. To do this, click **Start** on the task bar, select **Shut Down**, select **Restart the Computer**, and click **Yes**.
4	Contact your next level of support.

—End—

General protection faults

If you receive a general protection fault, perform the following procedure.

Troubleshooting general protection faults

Step	Action
	At the OAMP workstation
1	On the General Protection Fault window, click **Details**, noting the details about why this error occurred.
2	Simultaneously press Ctrl+Alt+Delete on your keyboard. The Close Program window appears. Note the programs that were active and exit all running programs.
3	Restart your OAMP workstation. To do this, click **Start** on the task bar, select **Shut Down**, select **Restart the Computer**, and click **Yes**.
4	Contact your next level of support.

—End—

OAMP workstation disk space is low

Description

A message indicating that your OAMP workstation is low on disk space appears when there is not enough disk space available on your workstation to create a new file. This message may be displayed when performing tasks such as:

- retrieving logs, alarms, or operational measurements (OMs) from the system
- running message signaling unit (MSU) trace collection
- backing up a data snapshot from the system to the OAMP workstation
- installing a new CD-ROM disc release
- adding a new site

Corrective action

Free up disk space by completing these procedures, as necessary:

- Empty the recycle bin.
- Run ScanDisk to determine whether problems exist on your OAMP workstation.
- Back up files.
- Delete MSU trace files for each configured site.
- Delete image files or data snapshots.

- Copy load image files or data snapshots to another drive on the workstation.

Emptying the recycle bin

Step	Action
	At the OAMP workstation
1	On the desktop, double-click the **Recycle Bin** icon.
2	If you do not need the files displayed in the recycle bin, click the **File** menu and select **Empty Recycle Bin**.
3	If you need any of the files displayed in the recycle bin, save the files to an appropriate area by selecting and dragging the files to that area.
4	Click the **File** menu and select **Empty Recycle Bin**.

—End—

Running ScanDisk

Step	Action
	At the OAMP workstation
1	On the desktop, double-click the **ScanDisk** icon.
2	Select the drive that contains the files and folders you want to check.
3	Click **Start**.

—End—

Backing up files

Step	Action
	At your OAMP workstation
1	Back up files from your OAMP workstation to floppy disks or a tape drive.

—End—

Deleting MSU trace files

Step	Action
	At the OAMP workstation
1	Open the MSU Trace File window. To do this, click **Network Mgmt** on the main menu, click **GWS/MSU Trace** on the Network Mgmt window, and click **MSU Viewer** on the SS7 GWS/MSU Trace window.
2	In the Trace Files list, select the MSU trace files you want to delete and click **Delete**.

—End—

Deleting image files or data snapshots

Step	Action
	At the OAMP workstation
1	Open the File Manager window. To do this, click **Administration** on the main menu and click **File Manager** on the Administration window.
2	In the Source list, select the drive on your OAMP workstation on which the files reside.
3	A list of snapshots and a description of each appears below the Snapshot and Description boxes.
4	Select the file(s) you want to delete and click Delete. (Do not delete image files or data snapshots that are designated for the alternate boot server.)

—End—

LAN-to-LAN/Dialup connection failed

Description

This section provides information to help you determine why your remote access connection failed.

ATTENTION
This issue applies if your system RAS is a Shiva LAN Rover.

Corrective action

Corrective actions vary according to the particular situation. The following sections list several possible situations and their appropriate actions.

No Dial-tone

If there is no dial tone for your connection, perform the following procedure.

Troubleshooting no dial-tone

Step	Action
	At the OAMP workstation
1	On the Communications Applications Module (CAM) shelf, check the phone line to your remote access server (RAS) (2 port or 8 port) and reconnect any disconnected lines.
2	If the phone line is connected, contact your next level of support.

—End—

Users disconnected

If the users become disconnected, perform the following procedure.

Troubleshooting users disconnected

Step	Action
	At the OAMP workstation
1	Try to reconnect to the system.
2	Check your modem cables and connections, ensuring they are properly installed and connected.
3	Check your networking software and connections to ensure they are properly installed and functioning.
4	Check cables connecting your computer to the network.
5	Access the Shiva online troubleshooting documentation and complete applicable procedures.
6	If you are still experiencing connection problems, contact your next level of support.

ATTENTION

If the GUI was active when you were disconnected, you may need to log in again.

—End—

Local device fails

Description

Connectivity has been lost on a device on your LAN.

This condition can be caused by the following:

- Cables to the specified device are improperly connected or damaged.
- The IP address of the specified device does is incorrect.
- The specified device is powered off or is faulty.

Corrective action

Once you determine the cause of the failure, perform the procedures that correspond to that cause:

- OAMP workstation/alternate boot server failure - Connectivity is lost between your OAMP workstation or alternate boot server and both RTC system nodes. This can be caused by the following: Your workstation is powered down, an Ethernet hub failure on your workstation occurred, or the cable between your workstation and the Ethernet hub is disconnected or damaged.
  - — inspect the OAMP workstation
  - — inspect the cables
  - — view the logs
  - — inspect the Ethernet hub
- Ethernet hub failure/split network failure - Connectivity is lost between the RTC system node in slot 12 and the devices on Hub_2 while maintaining connectivity to the devices on Hub_1, and connectivity is lost between the RTC system node in slot 15 and the devices on Hub_1 while maintaining connectivity to the devices on Hub_2. This can be caused when the cable between Hub_1 and Hub_2 is faulty.
  - — view the logs
  - — inspect the cables
  - — check the port
- RAS failure -- Connectivity is lost between both RTC system nodes and the RAS.
  - — inspect the cables
  - — check the RAS
- Real-time Controller (RTC) system node failure - Connectivity is lost between the RTC system node in slot 12 (RTC12) or slot 15 (RTC15) and all devices on the LAN.

ATTENTION
Perform the procedures for both the RTC12 and the RTC15.

— inspect the cables

— check Hub_1

Inspecting the OAMP workstation

Step	Action
	At the OAMP workstation
1	Ensure that your workstation has power and is turned on.
2	Ensure that your workstation is functioning properly. If it is not, correct any problems and visually inspect the cables, as described in the next section.

—End—

Inspecting the cables

Step	Action
	At the OAMP workstation
1	Visually inspect the cables to determine whether any cables are disconnected or damaged.
2	If any cables are disconnected or damaged, reconnect or replace them.
3	If all cables are connected properly, view the Logs window, as described in the next section.

—End—

Viewing the logs

Step	Action
	At the OAMP workstation
1	Determine if both RTC system nodes generated logs indicating that connectivity has been lost to your workstation/alternate boot server.
2	If logs are displayed, check the Ethernet hub, as described in the next section.

—End—

Inspecting the Ethernet hub

Step	Action
	At the OAMP workstation
1	Ensure that the Ethernet hub is powered on. If it is not, correct.
2	If the Ethernet hub still does not function, contact your next level of support.

—End—

Checking the port

Step	Action
	At the OAMP workstation
1	Access another port for the phone line.
2	If this failure is not corrected, contact your next line of support.

—End—

Checking the remote access system (RAS)

Step	Action
	At the OAMP workstation
1	Ensure that the RAS is powered on. If it is not, correct.
2	If the hub still does not function, contact your next level of support.

—End—

Inspecting Hub_1

Step	Action
	At the OAMP workstation
1	Ensure that Hub_1 is powered on. If it is not, correct.

2 If the hub still does not function, contact your next line of support.

—End—

OAMP workstation disaster recovery

Description

The programs and data stored on your OAMP workstation can be lost or damaged in a number of ways. Equipment damage, such as hard drive failure, data loss due to a computer virus, or user error are among the most common causes of data loss.

Use this disaster recovery operation when Windows will not start on your OAMP workstation or when your hard drive fails and your OAMP workstation cannot access stored data.

Corrective action

CAUTION
This procedure erases all files on your workstation. Make sure that you have a current data backup before you begin the procedure.

If you need to perform a disaster recovery operation on your OAMP workstation, perform the following procedure.

ATTENTION
Nortel Networks recommends that you format the hard drive of the OAMP workstation before you complete the restore steps. A reformat of the hard drive prevents the spread of computer viruses or continuation of issues that may have been affecting the workstation.

Performing a disaster recovery operation

The following procedures describe how to perform disaster recovery operations from a Windows-based OAMP workstation and a Solaris-based OAMP workstation.

Performing a disaster recovery operation from a Windows-based OAMP workstation

Step	Action

At the Windows-based OAMP workstation

1 Insert the disaster recovery CD-ROM shipped with your workstation into the CD-ROM drive. Due to licensing issues, each CD-ROM is specific to the workstation it is shipped with.

2 Reboot the workstation. The Symantec Ghost program starts, and restores the workstation to its original "as shipped" configuration. A DOS prompt appears when this step is complete.

This procedure takes approximately five minutes.

3 Remove the disaster recovery CD-ROM from the CD-ROM drive. Return the CD-ROM to its regular storage place.

4 Reboot the workstation. Windows 2000 starts.

5 A popup message prompts you to reboot the workstation a second time. Reboot the workstation.

6 Insert the tape containing your most recent data backup.

7 Double-click the **Backup Exec** icon on the desktop if you are running a Veritas program, or the Colorado Backup II icon if you are running a Colorado program.

8 Select **Restore files** using the Restore Wizard.

9 Click **OK**.

10 Click **Next**.

11 Select from media in the device.

12 Click **Next**. The workstation loads the information from the backup tape.

13 Select the backup date and time for the data that you want to restore.

14 Click **OK**. The workstation loads the information from the backup tape.

15 Click the check box next to the **C:** drive. All other boxes on the interface become checked.

16 Click **Next**.

17 Click **Next** a second time.

18 Select **Always** replace the file on my computer.

19 Click **Start**.

20 A popup message appears to make sure the correct backup tape is inserted. Click **OK**. The backup data restore process begins. The

system may generate a message indicating some files could not be replaced because they are in use. The files will be replaced when the workstation is rebooted.

This procedure takes approximately 15-20 minutes.

21 Click **OK**.

22 A popup message prompts you to reboot the workstation. Reboot the workstation.

23 The disaster recovery procedure is complete.

—End—

Performing a disaster recovery operation from a Solaris-based OAMP workstation

Step	Action
	At the Solaris-based OAMP workstation
1	Insert the Solaris disaster recovery CD shipped with your workstation into the CD-ROM drive and recover the Solaris operating system. Refer to SUN documentation for the system recovery procedure.
2	When the Solaris OS is recovered, remove the disaster recovery CD from the CD-ROM drive and return it to its regular storage location.
3	Install the ABS into the system. Refer to ABS Specification and User Guide documentation for the installation procedure.
4	Insert the CD-RW containing the USP data that you want to restore into the CD-ROM drive.
5	Refer to Administration: Restore Operations, section "Performing a restore operation from a backup CD-RW" in USP Security and Administration documentation for restore USP data.
6	You have completed this procedure.

—End—

Activate the Paths for Each ASP

Complete this procedure for each ASP.

Step	Action
1	Identify the affected ASP in the Alarms window, click the **Alarms** banner.
2	Access the ASP Administration window, click **Configuration>ips7>application-server-process-path**. All provisioned ASPs are listed in the ASP Records list, near the bottom of the window.
3	Click on the name of the ASP you want to activate. All data relating to this ASP automatically appears. You can also find the ASP by entering the ASP name in the **ASP Name** list and clicking **Find by Name**. If you are unsure of the ASP name, scroll through the list.
4	Click **Up** on the ASP Status/Actions portion of the ASP Administration window to activate the paths in this ASP.
5	Monitor the ASP Path Status list to determine whether any paths in this ASP become active.

If:	Do:
None of the paths become active	Continue this procedure at step 6.
Some of the paths become active	Go to the *Review the Logs for ASP Path Failures* section.
All the paths in the ASP become active	This procedure is complete.

Step	Action
6	Deactivate and activate this ASP (click **Down** on the ASP Status/Actions portion of the ASP Administration window; wait several seconds, then click **Up**).
7	Monitor the ASP Path State list to determine whether any paths in this ASP become active.

If:	Do:
None of the paths become active	Go to the *Review the Logs for ASP Path Failures* section.

If:	Do:
Some of the paths become active	Go to the *Review the Logs for ASP Path Failures* section.
All the paths in the ASP become active	This procedure is complete.

—End—

Activate a link

Activating a link

Step	Action

At the OAMP workstation

1 Click **Fault>alarm** on the main menu, click **Realtime** and identify the affected Link in the Alarms window.

2 Access the SS7 MTP Link Administration window. To do this, click **Configuration>mtp>link**.

3 To view a specific linkset, click **Search** and provide the following criteria.

Criteria	Selection
Field	linkset-name[1]
Condition	equal
Value	<the linkset name>
Records	100
1.If the linkset name is not known, either choose another Selection or modify the Condition and Value criteria.	

4 Click **Retrieve**.

5 Click on the selected Link and click **Activate** .

6 Monitor the Activation State box to determine whether any links in this linkset become active.

If:	Do:
the link did not become active	Continue this procedure at step 7.
the link became active	This procedure is complete.

7 Deactivate and activate the link (click **Deactivate** at the top of the window; wait several seconds, then click **Activate**).

8 Monitor the Activation State box to determine whether any links in this linkset become active.

If:	Do:
the link became active	This procedure is complete.
some, or none, of the links became active	Perform procedure, "Reviewing the logs for link failures" (page 183).

—End—

Activate the Links in Each Linkset

Complete this procedure for each linkset.

Activating the links in each linkset

Step	Action

At the OAMP workstation

1 Click **Fault>alarm** on the main menu, click **Realtime** and identify the affected Linkset in the Alarms window.

2 Access the SS7 MTP Linkset Administration window. To do this, click **Configuration>mtp>linkset**.

3 To view a specific linkset, click **Search** and provide the following criteria.

Criteria	Selection
Field	linkset-name[1]
Condition	equal
Value	<the linkset name>
Records	100
1.If the linkset name is not known, either choose another Selection or modify the Condition and Value criteria.	

4 Click **Retrieve**.

5 Click on the selected Linkset and click **Activate** .

6 Monitor the Activation State box to determine whether any links in this linkset become active.

If:	Do:
None of the links become active	Continue this procedure at step 7.
Some of the links become active	Go to the procedure "Reviewing the logs for link failures" (page 183).
All the links in the linksets become active	This procedure is complete.

7 Deactivate and activate the linkset (click **Deactivate** at the top of the window; wait several seconds, then click **Activate**).

8 Monitor the Activation State box to determine whether any links in this linkset become active.

If:	Do:
All the links in the linkset become active	This procedure is complete.
Some, or none, of the links become active	Go to the procedure "Reviewing the logs for link failures" (page 183).

—End—

Load a System Node

To load or reload a system node, perform the following procedure.

Loading a system node

Step	Action
	At the OAMP workstation
1	Open the affected system shelf window. To do this, click **Configuration>platform>node**.
2	To view the CAM shelf icon, click **Graphical View**.
3	Double-click the icon for the affected system node. The Administration panel appears.
4	If the system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.
5	Click **Load**. Wait for the system node to enable and click **Unlock** (with confirmation) to ensure the system node returns to full service.
6	If the affected system node was an IP link system node, determine if all ASPs are back in service. If any ASPs are still out of service, activate the paths for each ASP. See the Configuration guide for more information.
7	If the affected system node was an SS7 link system node, determine if all linksets are back in service. If any linksets are still out of service, Activate the links. See the Configuration guide for more information.
8	If the system node does not return to full service, perform the procedure to *Reseat Cards in System Nodes* in this section and repeat this procedure.

—End—

Reboot the Link System Node

Before a SS7 Link system node can be recovered, you must ensure at least one CC system node is enabled.

Rebooting the link system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node** to open the affected system shelf window.
2	Click **Graphical View** to view the CAM shelf icon.
3	Double-click the icon for a CC system node. The associated provisioning and maintenance window appears.

If the operational-state is:	Do:
disabled	step 4.
enabled	step 5.

4	Double-click the icon for the other CC system node. The associated provisioning and maintenance window appears.

If the operational-state is:	Do:
disabled	perform the procedure *Recover a CC System Node*.
enabled	step 5.

If both CC system nodes were disabled and you just recovered one, the system automatically recovers all application system nodes that are not offline. You can wait several minutes for the application system nodes to recover and then view the Alarms window to determine whether all have recovered, or you can begin recovering the application system nodes immediately.

5	Double-click the icon for the affected SS7 Link system node.
6	If the system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.
7	Click **Load**. Wait for the system node to enable and click **Unlock** (with confirmation) to ensure the system node returns to full service.

8 If the system nodes does not enable, proceed to the "Replacing mission cards or TMs in system nodes" (page 176)procedure.

9 If the SS7 Link system node enables but the links do not recover, proceed to the"Replacing mission cards or TMs in system nodes" (page 176) procedure.

—End—

Reload the RTC System Node

Reloading the affected RTC system node

Step	Action

At the OAMP workstation

1 Open the affected system shelf window. To do this, click **Configuration>platform>node**.

2 To view the CAM shelf icon, click **Graphical View**.

3 Double-click the icon for the appropriate RTC system node. The Administration panel appears.

If the RTC system node is:	Do:
active [1]	step 4.
inactive	step 5.

1. If this alarm is raised on the active RTC system node, a SWACT operation automatically performs if the inactive RTC system node is enabled and unlocked.

4 Click **SWACT**. At the confirmation prompt, click **Yes**.

Wait for the switch of activity to complete.

5 If the system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

6 Click **Load to download the boot image and re-initialize and enable the RTC system node**.

Wait for the system node to enable.

7 Click **Unlock**. At the confirmation prompt, click **Yes**.

If the alarm:	Do:
did not clear	step 8.
cleared	step 9.

8 Contact your next level of support.

9 The procedure is complete.

—End—

Replacing a power filter module

DANGER
Wait 30 seconds after the CAM is turned off (step 2 of the following procedure) before proceeding with subsequent steps in this procedure. This precaution allows the internal capacitors to discharge, and eliminates a electrocution hazard to operating company personnel.

CAUTION
Do not turn on the CAM power switch until 30 seconds have elapsed since the CAM was turned off. This will prevent damage to the power filter module.

Removing the power filter

Step	Action
	At the office power distribution panel
1	Turn off the breaker for the CAM under service.
	At the CAM power feed
2	Turn the CAM power switch to OFF.
3	Wait 30 seconds to allow capacitors to discharge.
4	Remove the six screws that secure the power filter module.
5	Remove the power filter module by pulling it out of the drawer.

—End—

Installing the replacement power filter

Step	Action
	At the CAM power feed
1	Slide the new power filter module into the drawer.
2	Replace the screws that secure the power filter module.
	At the office power distribution panel

3 Turn on the breaker for the CAM under service.

At the CAM power feed

4 Turn the CAM power switch to ON.

—End—

Replace an RTC mission card

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Replacing an RTC mission card

Step	Action

At the USP chassis

1 Press the Lamp Test buttons located on the front CC cards at slot 1 and 18, and rear of slots 1 and 18 of the CAM shelf to ensure all LEDs are working properly.

At the USP GUI

2 Click **Configuration>platform>node**.

3 Click the appropriate CAM shelf icon.

4 Click the icon for the affected RTC system node. The associated provisioning and maintenance window appears.

If	Do
the RTC system node is active	step 5
the RTC system node is not active	step 6

5 Click **SWACT**.

6 Use the following table to determine your next step.

If	Do
the RTC system node is locked	step 8
the RTC system node is not locked	step 7

7 Lock the RTC system node as follows:

a. Click **Lock**.

b. Select **Yes**.

8 Offline the RTC system node as follows:

a. Click **Offline**.

b. Select **Yes**.

c. Select **OK**.

d. Select **OK**.

At the UPS chassis

9 Press outward on the top and bottom latches of the RTC card to release it from the CAM shelf. Two audible clicks can be heard when the card is released completely.

10 Note the PEC label on the RTC card you just removed.

11 Obtain a new RTC card, verify it has the correct PEC label, and ensure the top and bottom latches are in the outward position.

ATTENTION
If the new RTC card has a different PEC than the one you are replacing, you will be required to change the PEC later in this procedure before loading the card.

12 Note the Ethernet ID address on the front of the new RTC card.

ATTENTION
You will be required to edit the bootp entries for the new RTC card later in this procedure.

13 Position the top and bottom latches of the new RTC card facing you, and gently slide the RTC card into the card guide of the one you removed, seating the bottom of the card into the card guide and then the top.

14 Apply pressure to the faceplate until you feel resistance.

15 Snap the top and bottom latches of the RTC card inward, toward one another. Two audible clicks can be heard when the card is seated properly.

At your workstation

16 Use the following table to determine your next step:

If	Do
the PEC of the new RTC card is the same as the PEC of the old RTC card (noted in step 10)	step 19
the PEC of the new RTC card is different from the PEC of the old RTC card (noted in step 10)	step 17

17 Modify the PEC for the RTC card through the USP GUI as follows:

a. Click **Configuration>platform>node**.

b. Click the **Graphical View** tab.

c. Click on the RTC Card list and select the appropriate PEC from the pull-down menu. If you need to type in a PEC, place your cursor inside the box.

d. Click **Modify**.

18 Set the new RTC software load as follows:

a. At the main USP GUI menu, click **Administration**.

b. In the Admin window, click **ABS Settings**.

c. Select the new software load listed in the Alternate Boot Loads field.

For NTST11BA, select ss7rtc_ppc750_xx_xx_xx_xx.

For NTST11DB, select ss7rtc_pp5_xx_xx_xx_xx.

d. Click **Apply**.

e. Click **Close**.

19 Edit the bootp entries for the new RTC according to whether the Alternate Boot Server (ABS) is on a PC, the CS 2000 Management Tools server, or on the Sun Workstation at the USP:

ATTENTION
If the ABS is on a customer-supplied Bootp server, use the customer-supplied documentation to edit the bootp entries.

If	Do
the ABS is on a PC	step 20

If	Do
the ABS is on the CS 2000 Management Tools server	step 21
the ABS is on the Sun Workstation at the USP	step 22

20 Edit the bootp entries for the new RTC card on a PC as follows:

a. Click the **Distinct BOOTP Server** button on the taskbar to maximize the Distinct BOOTP Server window.

b. Click the **Configure** menu, select **Administrator** and then **Login** to display the Distinct BOOTP Login window.

c. Enter your administrator password in the **Enter the administrator password** field and click **OK** to log in to the server.

The Distinct BOOTP Login window closes.

d. Click the **Configure** menu and select **Server** to display the Configure BOOTP window.

e. Select the **Addresses** tab window.

f. Remove the bootp entry for the RTC card you removed.

g. Enter the new Ethernet Hardware Address (MAC). This is the address you noted in step 12.

h. Enter the IP address (software) for the new RTC.

i. Enter the boot file as follows:

If you replaced the RTC card in slot 12, enter /c/ntssgusp/abs/sites/<sitename>/rtc1/rtcboot

If you replaced the RTC card in slot 15, enter /c/ntssgusp/abs/sites/<sitename>/rtc2/rtcboot

j. Click **Add**.

k. Click **Apply**.

21 Edit the bootp entries for the new RTC card on the CS 2000 Management Tools server as follows:

a. Open a Telnet session to the CS 2000 Management Tools server by typing

```
telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the CS 2000 Management Tools server

b. When prompted, enter the maint user ID and password.

c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d. When prompted, enter the root password.

e. Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

f. Enter the number next to the "Configuration" option in the menu.

g. Enter the number next to the "Bootp Configuration" option in the menu.

h. Enter the number next to the "bootp_add" option in the menu.

i. When prompted, enter the bootfile value for bootp entry.

For RTC 12, type:

```
/data/usp/ntssgusp/abs/sites/<sitename>/rtc1/rtcboot
```

For RTC 15, type:

```
/data/usp/ntssgusp/abs/sites/<sitename>/rtc2/rtcboot
```

j. When prompted, enter the gateway IP address for bootp entry.

k. When prompted enter a period (.) for the home directory location for bootp entry.

l. When prompted, enter ethernet for the hardware type for bootp entry.

m. When prompted, enter the Ethernet ID address of the new RTC card. This is the address you noted in step 12.

n. When prompted, enter the RTC (slot 12 or 15) IP address for bootp entry.

o. When prompted, enter the CS 2000 Management Tools server IP address for bootp entry.

p. When prompted, enter the subnet mask value for bootp entry.

q. Review the settings, and if acceptable, confirm them by typing

```
ok
```

and pressing the Enter key.

r. Exit each menu level of the command line interface to return to the command prompt.

s. Log out of the server.

t. Close the Telnet session.

22 Edit the bootp entries for the new RTC card on the Sun Workstation as follows:

a. Open a terminal window.

b. When prompted, change directories by typing

```
cd /usr/sadm/admin/bin
```

and pressing the Enter key.

c. When prompted, open the DHCP Manager dialog box by typing

```
./dhcpmgr
```

and pressing the Enter key.

The DCHP Manager dialog box appears.

d. Select the **Addresses** tab window.

e. Click the RTC card that you are changing.

The RTC card you are changing is highlighted.

f. Note all the address parameters associated with the RTC card you are changing including the IP address, the associated macro, and so on.

g. Click the **Edit** menu and select **Delete**.

h. Confirm that the RTC card you are changing is deleted.

i. Click the **Edit** menu and select **Create**.

j. Enter the **IP Address** that you noted in step f and select the Configuration Macro for the RTC card you are changing.

k. Select the **Lease** tab window.

l. Enter the new Ethernet Hardware Address (MAC) in the **Client ID** field. This is the address you noted in step 12. In the **Client ID** field, the MAC address must be proceeded by the digits 01.

m. Select **Reserved**, **Permanent assignment**, and **Assign only to BOOTP clients**.

n. Click **OK**.

o. Close the DHCP Manager dialog box.

23 On the associated system node provisioning and maintenance window, click **Load** and wait for the system node to enable, click

Unlock to ensure the system node returns to full service, and click **Close**.

24 On the shelf_name window, ensure that the LED indicator is lit for the system node and click **Close** twice.

You have completed this procedure.

—End—

Replacing Mission Cards or TMs in System Nodes

CAUTION
The corresponding redundant node of the affected node must be in-service while performing this procedure. An attempt to perform this procedure on a stand-alone node may result in service degradation.

CAUTION
Wear wrist straps and use standard antistatic precautions.

Replacing mission cards or TMs in system nodes

Step	Action
	At the USP chassis
1	Obtain new mission cards or TMs, verify they have the correct PEC labels, and ensure the top and bottom latches are in the outward position. If you are replacing a V.35 TM, check the configuration of the DTE/DCE modules on the new TM card. For more information, see "Verify the Operational Mode of Each V.35 TM Port" (page 185). If you are replacing an RTC mission card, perform procedure "Replacing an RTC mission card" (page 169). If the new mission card and TM have different PECs than the ones you are replacing, you must change the PEC and the boot-image in the Provisioning and Maintenance window before loading the card. If you need to change the PEC of the SCSI card or TM, refer to Configuring an RTC System Node. For more information, see *USP Configuration Management* (NN10093-511).
	At the USP GUI
2	Click **Menu>Fault>log** and select the **Realtime** tab.
3	Click **Start** to monitor the USP logs.
4	If you are replacing a Link card, inhibit and deactivate the links on that card. For more information, see *USP Configuration Management* (NN10093-511).

5 If you are replacing an IPLink card, take down the AS Paths associated with that card. For more information, see *USP Configuration Management* (NN10093-511).

6 Open the affected system shelf window. To do this, click **Configuration>platform>node**.

7 To view the CAM shelf icon, click **Graphical View**.

8 Double-click the icon for the affected system node (RTC, CC, or application). The associated provisioning and maintenance window appears.

9 If the system node you are replacing is not locked or out of service, click **Lock**. At the confirmation prompt, click **Yes**.

10 Click **Offline**. At the confirmation prompt, click **Yes**.

At the USP chassis

11 Before you replace a CC mission card, unseat and disconnect its corresponding OC-3 TM.

12 Before you replace a SCSI Disk card, unseat its corresponding RTC mission card and then unseat the SCSI Disk card.

13 Before you unseat a TM, remove its connector(s) by unscrewing the thumbscrews on the top and bottom of each connector. Gently pull off the TM cable connector(s).

14 Press outward on the top and bottom latches of the mission card or TM to release it from the CAM shelf. Two audible clicks can be heard when the mission card or TM is released completely.

15 Grasp the top and bottom latches of the mission card or TM and gently pull it toward you to remove it from the CAM shelf.

16 Position the top and bottom latches of the new mission card or TM facing you, and gently slide the mission card or TM into the card guide of the one you removed, seating the bottom of the mission card or TM into the card guide and then the top.

17 Apply pressure to the faceplate until you feel resistance.

18 Snap the top and bottom latches of the mission card or TM inward, toward one another. Two audible clicks can be heard when the mission card or TM is seated properly.

19 After you replace the TM, plug in the TM connector(s) and turn the thumbscrews on the top and bottom of the connector(s) to tighten.

20 If you replaced a CC mission card, remember to reseat and reconnect its OC-3 TM.

21 If you replaced a SCSI Disk card, remember to reseat its RTC mission card.

22 At the front and rear of the CAM shelf on the CC node, press the white Lamp Test buttons. If the LEDs do not light for the system node you just replaced, ensure the mission card and TM are seated properly by performing steps 11to 21again.

At the USP GUI

23 On the system node provisioning and maintenance window, click **Load** and wait for the system node to enable, click **Unlock** to ensure the system node returns to full service, and click Close.

24 If you are replacing a Link card, activate and uninhibit the links on that card. For more information, see *USP Configuration Management* (NN10093-511).

25 If you are replacing an IPLink card, bring the AS Paths associated with that card back up. For more information, see *USP Configuration Management* (NN10093-511).

26 After the card has been replaced and the card has been successfully loaded, click **Realtime** to check the log-severity field. If the "log-swerr" or "log-trap" logs are displayed for the same system node, contact your next-level support.

27 Let the card soak for one to five minutes after it has been successfully loaded and unlocked. Monitor the USP logs using the Realtime tab during this period.

28 After the successful soak period, click **Realtime** and then click **Stop** to stop the realtime log monitoring.

29 On the Graphical View, ensure that the LED indicator is lit for the system node.

30 Click **Fault>alarm** on the main menu. The Alarms window appears. Click **Realtime**. If this alarm is still displayed for the same system node, contact your next-level support.

—End—

Replace the Fan Tray

CAUTION
Wear wrist straps, and use standard antistatic precautions.

Replacing the fan tray

Step	Action
	At the USP chassis
1	Locate the air grill on the front of the affected CAM shelf.
2	Using a flat blade screwdriver, loosen the two screws on the air grill by turning counter-clockwise 3/4 turn.
3	Gently pull the air grill toward you to remove it.
4	Remove the fan tray. Grasp the lower edge of the fan tray, placing your thumbs on the two spring-release latches. Press the two latches inward and up, gently pulling the fan tray toward you.
5	Insert the new fan tray. Lift the new fan tray and slide into the CAM shelf until seated properly. Two audible clicks can be heard when the fan tray is seated properly.
6	Position the air grill on the fan assembly.
7	Using a flat blade screwdriver, turn the two screws on the air grill clockwise 3/4 turn.
8	View the Alarms window by clicking Alarms on the main menu.
9	If the alarm condition persists, replace the TMs of the CC system nodes.

—End—

Reseat the Fan Tray

CAUTION
Wear wrist straps, and use standard antistatic precautions.

Reseating the fan tray

Step	Action
	At the USP chassis
1	Locate the air grill on the front of the affected CAM shelf and, using a flat blade screwdriver, loosen the two screws on the air grill by turning counter-clockwise 3/4 turn.
2	Grasp the lower edge of the fan tray, placing your thumbs on the two spring-release latches.
3	Press the two latches inward and up, gently pulling the fan tray toward you.
4	Slide the fan tray back into the CAM shelf until seated properly. Two audible clicks can be heard when the fan tray is seated properly.
5	Position the air grill on the fan assembly.
6	Using a flat blade screwdriver, turn the two screws on the air grill clockwise 3/4 turn.
7	View the Alarms window by clicking **Alarms** on the main menu.
8	If the alarm condition persists, then replace the fan tray.

—End—

Reseat Cards in System Nodes

CAUTION
Before handling hardware, wear wrist straps and use standard antistatic precautions.

Reseating cards in system nodes

Step	Action

At the OAMP workstation

1 Open the affected system shelf window. To do this, click **Configuration>platform>node**.

2 To view the CAM shelf icon, click **Graphical View**.

3 Double-click the icon for the intended CC system node. The Administration panel appears.

If the CC system node is:	Do:
online	step 4.
offline	step 6.

4 If the CC system node is not locked, click **Lock**. At the confirmation prompt, click **Yes**.

5 Click **Offline**. At the confirmation prompt, click **Yes**.

6 Disconnect the OC-3 TM corresponding to the mission card you are reseating. Remove the connectors attached to it by unscrewing the thumbscrews on the top and bottom of the connectors. Gently pull off the cable connectors.

7 Press outward on the top and bottom latches of the mission card and TM to release them from the CAM shelf.

8 Grasp the top and bottom latches of the mission card and TM and gently pull them toward you to remove them from the CAM shelf.

ATTENTION

If the mission card or TM you are reseating is in an application system node or an SS7 link system node and the node is equipped with a V.35 TM, check the operational mode of the ports as described in "Verify the Operational Mode of Each V.35 TM Port" (page 185).

9 Ensure the top and bottom latches of the mission card or TM are in the outward position by pressing outward on each latch.

10 Position the top and bottom latches facing you of the mission card or TM, and gently slide the bottom of the card into the card guide first, then slide in the top.

11 Apply pressure to the faceplate until you feel resistance.

12 Snap the top and bottom latches of the mission card or TM inward (toward one another). Two audible clicks can be heard when the mission card is seated properly.

13 After you reseat the TM, plug in its connectors and turn the thumbscrews on the top and bottom of the connectors to tighten them.

14 On the front and rear of the CAM shelf, press the Lamp Test buttons.

15 If the LEDs do not light, replace the mission card or TM of the affected system node.

16 If you reseated the mission card and TM on the CC system node, click **Load** (in the CC system node Administration view) and wait for the system node to enable. Then click **Unlock** to ensure the system node returns to full service. If the system node does not enable, perform procedure "Replacing mission cards or TMs in system nodes" (page 176).

17 If the LEDs light, this procedure is complete.

—End—

Review the Logs for Link Failures

Reviewing the logs for link failures

Step	Action
	At the OAMP workstation
1	Access the Logs window. To do this, click **Fault>log** on the main menu.
2	On the Logs window, identify all link failure logs that correspond to the linksets you tried to activate. To do this, click the **Search** view, click ... and click on an appropriate time frame, click **Select**, and click **Retrieve**.
3	If *Stop Received* appears, proceed to the "Verifying all signal link test (SLT) settings" (page 71) section.
4	If you are reviewing logs for SS7 IP High Speed links and the log information indicates a hardware problem, proceed to "Inspecting the cables for SS7 IP High Speed Link failures" (page 84).
5	If any of the following information appears, proceed to "Inspecting cables and transmitter equipment" (page 71). • SIO received • SIOS received • Abnormal FIBR/BSNR • T7 expired • T6 expired • SUERM
	—End—

Verify the IP address and Port

Verifying the IP address and port

Step	Action
	At the OAMP workstation
1	Call the remote site to verify that the IP address and port for each path on your USP matches the IP address and port settings on the remote site.
2	To view the IP address and port assigned to a path, click **Configuration>IPS7>application-server-process-path**.
3	Note the IP address displayed in the *dest-ipaddr* box and the port displayed in the *dest-port* box.
4	If the IP address and port of the path and the settings at the remote site do not match, correct the settings and perform this procedure again, starting from the Enable all Disabled IP Link System Nodes section. If the IP addresses match, proceed to the Reboot the IP Link System Node section.

—End—

Verify the Operational Mode of Each V.35 TM Port

Ensure that the operational mode of each V.35 TM port is compatible with the operational mode of the remote site. For example, if the operational mode of a TM port is DTE, the operational mode of the remote site must be DCE.

CAUTION
Wear wrist straps and use standard antistatic precautions.

After removing a V.35 TM to reseat it and before installing a new V.35 TM, check the operational mode of the ports by performing the following procedure.

Step	Action
1	Locate the plug-in module on the TM associated with the port that you want to check.
2	The lower edge of the TM card contains the text DTE/DCE and an arrow. Each plug-in module is labelled DCE on one end and DTE on the other end. The orientation of each plug-in module with respect to the arrow on the TM card determines the operational mode of the port.
3	Check that each port is configured correctly. If necessary, unplug the module associated with a port that you want to configure and plug it back into the TM card such that the correct end of the module aligns with the arrow on the TM card.

—End—

Verify the Point Codes (PCs) (Local and Remote)

Verifying the PCs (local and remote)

Step	Action
	At the OAMP workstation
1	Call the remote site to verify that the PC on your USP matches the PC on the remote site.
2	Click **Configuration>mtp>system-id** to access the System Identity window.
3	Note the PC displayed in the Point Code box.

If:	Do:
The PCs of the remote office and your USP do not match	Correct the point code and return to the Enabling System Nodes section.
The PCs match	Proceed to the procedure "Verifying the SLCs" (page 187).

—End—

Verify the SLCs

Verifying the SLCs

Step	Action
	At the OAMP workstation
1	Verify that the SLCs on your USP match those of the remote site. To do this, click **Configuration>mtp>linkset**. The SS7 MTP Linkset Administration window appears.
2	View the Linkset Status/Actions portion of the MTP Linkset Administration window, verifying that the SLCs set up for your USP match those of the remote site.
3	If the SLCs do not match, correct and perform this procedure again, starting from the Enable all Disabled SS7 Link System Nodes section. If the SLCs match, check the facilities at the remote site, correcting any problems, and perform this procedure again, starting from the Enabling System Nodes section. If problems are not reported at the remote site, proceed to the Perform BERT section in *USP Security and Administration* (NN10159-611).
	—End—

Number Portability (NP) and Service Location Register (SLR) Alarms

Application Database Manager, 5: NPAC Data Lost (Critical)

Description

This alarm occurs when the application database (DB) on a Number Portability Controller (NPC) system node loses external provisioning system data.

Corrective action

You must perform a bulk load operation to reload the application DB. To bulk load data to a local subsystem (LSS), perform the following procedure.

Performing a bulk load of data to a LSS

Step	Action

At the OAMP workstation

1 Open the SCCP Local Subsystems window. To do this, click **Configuration>SCCP>Local-Subsystem**.

2 To access a selected LSS, click **Search** and provide the following criteria.

Criteria	Selection
Field	lss-class[1]
Condition	equal
Value	<the lss class>
Records	100
1.If the lss class is not known or other search criteria are preferred, either choose another Field or modify the Condition and Value criteria.	

3 Click **Retrieve**.

4 Click the desired LSS from the *Retrieval Results*.

5 If the LSS is activated according to the *admin-state* box, click **Deactivate**.

6 Click the **LSS Instances** button.

7 Click the **Bulk Load** button.

8 Select **Full** from the Bulk Load Type list.

9 Enter the remote IP address in the **IP Address** box.

10 Enter the user ID in the **User ID** box. The remote site system administrator provides this information.

11 Enter the password in the **Password** box. The remote site system administrator provides this information.

12 In the **Remote File Path** box, enter the file name and full path for the file that will be downloaded to the USP.

Two files are transferred: a schema file and a data file. The schema file describes the structure of the larger data file and contains the file name of the data file.

ATTENTION
Contact personnel at the provisioning system site to ensure that this file is prepared.

13 Click **Start**.

The Bulk Load Status window opens. The Transfer field indicates the status of the FTP action from the provisioning system to the USP. The Import field indicates the status of the file conversion and database loading on the USP. The bulk load completes when the Transfer and Import fields both indicate 100 percent.

If your Application DB is populated with records from a single provisioning system database, the procedure is complete. Otherwise, go to step 14.

14 Repeat steps 6 to 13 for each provisioning system database that is used to populate your Application DB. You must select incremental when you specify the setting for the Bulk Load Type (step 8) each time.

—End—

Application Database Manager, 6: *application* Database Is Full (Minor)

Description

This alarm occurs when the Application DP contains the maximum number of records and an attempt is made to add another record.

Corrective action

To clear this alarm, complete the following procedure.

Clearing: *application* Database is Full alarm

Step	Action

At the OAMP workstation

1

If:	Do:
you are using an NP application	Modify the filtering criteria in the provisioning system for your USP, making the criteria more restrictive in selecting number portability (NP) records to be forwarded from the provisioning system. Refer to your provisioning system provider for the appropriate procedure.
you are using an SLR application	Remove unused records from the database or deploy another SLR node.

2 Complete the procedure "Performing a bulk load of data to a LSS" (page 188).

—End—

Application Database Manager, 7: *application* Database Is Corrupted (Critical)

Description

This alarm occurs when the Application DB manager detects a corruption in the Application DB.

Corrective action

The system typically clears this alarm automatically by transferring a good copy of the Application DB from another NPC or Number Portability Server (NPS) system node.

If the system cannot clear this alarm automatically, you must complete the procedure "Performing a bulk load of data to a LSS" (page 188).

Application Database Manager, 19: *application* LSS on the Active NPC is Deactivated (Minor)

Description

This alarm occurs when the LSS instance associated with the active NPC system node is in the deactivated administrative state. Deactivated LSSs cannot process updates from the provisioning system.

Corrective action

If this alarm is triggered while you are performing initial Application provisioning or a bulk load of the Application DB, no corrective action is necessary. Otherwise, complete the following procedure to clear this alarm.

Clearing: *application* LSS on the Active NPC is Deactivated.

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Ensure that both NPC system nodes are enabled and unlocked. Look for the icons for the NPC system nodes in the shelf_name window. An icon for an enabled and unlocked NPC system node has a green LED symbol at the top and does not have a lock symbol in it.

If both NPC system nodes are enabled and unlocked, go to step 8. Otherwise, go to step 3.

3 Click the icon for a disabled and/or locked NPC system node. The NPC system node Provisioning and Maintenance window opens.

If the NPC system node is:	Do:
disabled	go to step 4.
enabled	go to step 6.

4 Click **Lock**. If the NPC system node is already locked, go directly to step 5.

5 Click **Load**. Go to step 7.

6 Click **Unlock**.

7 Repeat steps 3 to 6 if the other NPC system node is not enabled and unlocked. Go to step 9.

8 Click the icon for an NPC system node.

9 Click **SWACT** to switch the active NPC system node.

If the SWACT operation is:	Do:
successful	go to step 12.
not successful (The LSS instance associated with the NPC system node has been manually deactivated.)	go to step 10.

10 Open the SCCP Local Subsystem window. To do this, click **Configuration>sccp>local-subsystem**.

11 Activate the LSS. To do this, complete the following steps:

a. Scroll through the LSS Records list near the bottom of the window to find the LSS that you want to activate.

b. Click this LSS.

c. Click **Activate** on the LSS Status portion of the window.

12 If the system clears the alarm, the procedure is complete. Otherwise, contact your next level of support.

—End—

Application Database Manager, 20: *application* Database Lost Synchronization (Minor)

Description

This alarm occurs when the Application database on an NPC or NPS system node loses synchronization with the databases on other NPC or NPS system nodes. While the database is unsynchronized, the Application subsystem instance is not available to handle Application query traffic.

Corrective action

The system automatically attempts to retrieve the missed database updates from the Application database on another NPC or NPS system node. When the database is resynchronized, the Application subsystem instance returns to the "allowed" state.

If the system does not clear the alarm automatically, or if you receive other Application DB Manager 20 alarms, contact your next level of support.

Application Database Manager, 27: *application* Database Timestamp Is Invalid (Critical)

Description

This alarm occurs when the creation timestamp for the Application DB on the affected Application system node references a date and time that is ahead of the date and time used on the USP. Since the creation timestamp is used in the synchronization of the Application DB between Application system nodes and the creation timestamp is not correct, the Application DB is declared invalid by the Application DB manager.

Corrective action

To clear this alarm, perform the following procedures, as necessary:

- Verify the data and time, see "Verifying the date and time" (page 193).
- Modify the date and time, see "Modifying the date and time information for the USP" (page 194).
- Perform a bulk load of data to an LSS, see "Performing a bulk load of data to a LSS" (page 188).

Verifying the date and time

Step	Action
	At the OAMP workstation
1	Click **Administration>date-time**.
2	If the date and time settings are not correct, complete the procedure "Modifying the date and time information for the USP" (page 194).
3	If the date and time settings for the USP are correct and both of the NPC system nodes are affected by this alarm, complete the procedure "Performing a bulk load of data to a LSS" (page 188).

ATTENTION

If the bulk load is successful but the alarm does not clear, contact your next level of support.

If the bulk load is not successful, perform the corrective action associated with the particular bulk load failure that occurred.

4	If the date and time settings for the USP are correct and only one of the NPC system nodes is affected by this alarm, the USP automatically clears this alarm.

—End—

Modifying the date and time information for the USP

Step	Action

At the OAMP workstation

1 Click **Administration>date-time**.

2 Click the **calendar** button on the date box and select the date.

3 Click the **clock** button on the time box and enter the local time.

4 If you need to modify the local time zone, click the **Time Zone** list. A world-wide list of time zones appears. Select your local time zone.

> **ATTENTION**
> The daylight savings time boxes are unavailable when the time zone you select does not use daylight savings time.

5 If you need to enable or disable the automatic system clock adjustment for daylight savings time, click the Adjust clock for daylight savings changes check box.

> **ATTENTION**
> If you are enabling the automatic system clock adjustment for daylight savings time for the first time, make sure to perform steps 6 to 11.

6 If you need to modify the starting month for daylight savings time, click the Start Month list. Select the month in which daylight savings time starts.

7 If you need to modify the starting day for daylight savings time, highlight the number in the Start Day box or click the up or down arrow buttons to the right of the box to enter the correct information.

8 If you need to modify the starting hour for daylight savings time, highlight the number in the Start Hour box or click the up or down arrow buttons to the right of the box to enter the correct information.

9 If you need to modify the ending month for daylight savings time, click the End Month list. Select the month in which daylight savings time ends.

10 If you need to modify the ending day for daylight savings time, highlight the number in the End Day box or click the up or down arrow buttons to the right of the box to enter the correct information.

11 If you need to modify the ending hour for daylight savings time, highlight the number in the End Hour box or click the up or down arrow buttons to the right of the box to enter the correct information.

12 If the alarm clears, the procedure is complete. Otherwise, contact your next level of support.

—End—

Application Database Manager, 31: Database Manager Goes into Failed State (Major)

Description

This alarm occurs when the database manager goes into a failed state. The card and the associated local subsystem instance (LSSI) remain out of service until the alarm is cleared.

The database manager can go into a failed state for one of the following reasons:

- A fatal error occurred when trying to access disk files.
- The user tried to change the LSS type while the card is in-service.
- The NPC or NPS card cannot communicate with the NPE cards in its chain.

Corrective action

To clear this alarm, perform the following procedures as necessary:

- Reload the NPx (either NPC, NPS, or NPE) card that raised the alarm, see "Loading the NPx system node" (page 195).
- Change the NPx card, see "Replacing the mission card or TM of the NPx system node" (page 196).

ATTENTION
Perform this procedure if the problem persists after reloading the card twice.

Loading the NPx system node

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

If the NPx system node is:	Do:
locked	go to step 5.
not locked	go to step 2.

2 Deactivate any LSS instance associated with this NPx system node. To do this, complete the following steps:

a. Open the Application Local Subsystem Instances window. Click **Network Mgmt** on the main menu. Click **Local SSNs** on the SS7 SCCP window.

b. Right-click on the desired instance in the LSS Instance Statuses section of the SCCP Local Subsystem window. Left-click on LSS Instances button. The Local Subsystem Instances window opens.

c. Scroll through the LSS Instance Records list, near the bottom of this window. Find the LSS Instance that you want to deactivate and click on it.

d. Click **Deactivate** on the LSS Instance Status portion of the window. Use **Deactivate All** to deactivate all of the instances.

3 Return to the NPx system node Provisioning and Maintenance window.

4 Click **Lock**.

5 Click **Load** and wait for the NPx system node to enable.

6 Click **Unlock** to ensure the system node returns to full service.

7 If the NPx system node does not return to full service, try to reload the card again. If the NPx node fails to load after the second attempt, replace the card. See the procedure "Replacing the mission card or TM of the NPx system node" (page 196).

—End—

CAUTION
Wear wrist straps, and use standard antistatic precautions.

Replacing the mission card or TM of the NPx system node

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click **Lock** on the NPx system node.

3 Click **Offline**.

At the USP chassis

4 Obtain a new mission card and PSE, verify they have the correct PEC labels, and ensure the top and bottom latches are in the outward position.

5 Before you unseat the TM, remove the connector(s) attached to it by unscrewing the thumbscrews on the top and bottom of each connector. Gently pull off the cable connector(s) for the TM.

6 Press outward on the top and bottom latches of the mission card or TM to release it from the CAM shelf. Two audible clicks can be heard when the mission card or TM is released completely.

7 Grasp the top and bottom latches of the mission card or TM and gently pull it toward you to remove it from the CAM shelf.

8 Position the top and bottom latches of the new mission card or TM facing you, and gently slide the mission card or TM into the card guide of the one you removed, seating the bottom of the mission card or TM into the card guide and then the top.

9 Apply pressure to the faceplate until you feel resistance.

10 Snap the top and bottom latches of the mission card or TM inward, toward one another. Two audible clicks can be heard when the mission card or TM is seated properly.

11 After you reseat the TM, plug in its TM connector(s) and turn the thumbscrews on the top and bottom of the connector(s) to tighten.

12 On the front and rear of the CAM shelf, press the Lamp Test buttons. If the LEDs do not light for the NPx system node you just replaced, ensure the mission card and TM are seated properly by unseating each and completing steps 5 to 11 again.

13 If the LEDs light, on the NPx system node Provisioning and Maintenance window, click **Load** and wait for the NPx system node to enable.

14 Click **Unlock** to ensure the NPx system node returns to full service.

15 If the NPx system node does not enable, contact your next level of support.

—End—

Application SMI, 12: No LSMS Connections Are Active (Minor)

Description

This alarm occurs when there are no active connections between the Local Service Management System (provisioning system) and an NPC system node, and the associated LSS instance is in an allowed state.

This alarm can also occur when one or both links from the provisioning system to the USP are down.

Corrective action

To clear this alarm, complete the following procedures, as necessary:

- Verify the provisioning system functional state, see "Verifying the provisioning system functional state" (page 198).
- Verify the user ID and password, see "Verifying the user ID and password" (page 198).
- Verify the TCP port number value, see "Verifying the TCP port number value" (page 199).
- Verify the network connectivity, see "Verifying the network connectivity" (page 199).

Verifying the provisioning system functional state

Step	Action
	At the OAMP workstation
1	Verify that the provisioning system is functioning correctly according to the procedures provided by your provisioning system provider.
2	If the alarm clears, the procedure is complete. Otherwise, go to the procedure "Verifying the user ID and password" (page 198).

—End—

Verifying the user ID and password

Step	Action
	At the OAMP workstation
1	If this alarm is only present for one of the NPC system nodes, the user ID and password settings are correct. Go to the procedure "Verifying the TCP port number value" (page 199). If this alarm is present for both of the NPC system nodes, go to step 2.

2 Click **Security>user-account**.

3 Check the user ID has a class range that includes Class 4.

4 From the User ID list, select the user ID for the associated provisioning system.

5 Click **Modify**.

6 Enter the password into the **User Password** box.

7 Enter the password from step 6 into the **Confirm User Password** box.

8 Click **Apply**.

9 Ensure that the user ID and password settings entered above are identical in the associated provisioning system.

10 If the alarm clears, the procedure is complete. Otherwise, go to the procedure "Verifying the TCP port number value" (page 199).

—End—

Verifying the TCP port number value

Step	Action

At the OAMP workstation

1 On the provisioning system GUI, verify that the TCP port number is set to 50080. Refer to your provisioning system provider's documentation for details on how to perform this check.

2 Correct the value, if it is other than 50080.

3 If the value is correct, or the alarm does not clear, go to the procedure "Verifying the network connectivity" (page 199).

—End—

Verifying the network connectivity

Step	Action

At the OAMP workstation

1 Perform a ping test to verify the network connectivity. To do this, complete the following steps:

a. From the UNIX terminal associated with the provisioning system, enter the following command:

```
/usr/sbin/ping <NPC_system_node_IP_address>
```

b. Once the ping test is complete, repeat this command using the IP address of the other NPC system node.

2 If both links pass the ping test, go to the section "Recover an NPC system node" (page 200) and recover both NPC system nodes.

If the ping test for either or both of these links fails, troubleshoot the network path between the NPC system node(s) and the provisioning system.

3 If troubleshooting the network path clears the alarm, the procedure is complete. Otherwise, refer to your provisioning system provider's troubleshooting procedures to validate that the provisioning system is configured correctly.

4 If all steps to clear the alarm fail, contact your next level of support.

—End—

Recover an NPC system node

To recover an NPC system node, complete the following procedures, as required:

- Enable a CC system node, see "Enabling a CC system node" (page 200).
- Load the NPC system node, see "Loading the NPC system node" (page 201).
- Reseat the mission card and TM, see "Reseating the mission card and TM" (page 202).
- Replace the mission card and TM, see "Replacing the mission card and TM" (page 204).

Before an NPC system node can be recovered, you must ensure that at least one CC system node is enabled on the same shelf. To do this, complete "Enabling a CC system node" (page 200).

Enabling a CC system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.

2 Click the appropriate CAM shelf icon.

3 Click the icon for a CC system node.

If the Operational State field displays:	Do:
Enabled	go to "Loading the NPC system node" (page 201).
Disabled	go to step 4.

4 Repeat steps 1 to 3 to determine whether the other CC system node is enabled.

If:	Do:
the other CC system node is enabled	go to "Loading the NPC system node" (page 201).
both CC system nodes are disabled	go to step 5.

5 Recover a CC system node as described in section "Recover a CC system node" (page 205), then go to step 6.

6 When a CC system node has been successfully recovered, load the NPC system node as described in "Loading the NPC system node" (page 201).

ATTENTION

If both CC system nodes were disabled and you just recovered one, the system automatically recovers all application system nodes that are not offline. You can wait several minutes for the application system nodes to recover and then view the Alarms window to determine whether all have recovered, or you can begin recovering the application system nodes immediately.

—End—

Loading the NPC system node

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click the appropriate CAM shelf icon.

3 Click the icon for the affected NPC system node. The NPC system node Provisioning and Maintenance window opens.

If the NPC system node is:	Do:
locked	go to step 7.
not locked	go to step 4.

4 Deactivate any LSS instance associated with this NPC system node. To do this, complete the following steps:

a. Open the Local Subsystem Instances window. Click Network Mgmt on the main menu. Click Local SSNs on the SS7 SCCP window.

b. Right-click on the desired instance in the LSS Instance Statuses section of the SCCP Local Subsystems window. Left-click on Instances button. The Local Subsystem Instances window opens.

c. Scroll through the LSS Instance Records list, near the bottom of this window. Find the LSS Instance that you want to deactivate and click on it.

5 Return to the NPC system node Provisioning and Maintenance window.

6 Click **Lock**.

7 Click **Load** and wait for the NPC system node to enable.

8 Click **Unlock** to ensure the system node returns to full service.

9 If the NPC system node does not return to full service, reseat the mission card and TM of the NPC system node, as described in "Reseating the mission card and TM" (page 202).

—End—

CAUTION
Wear wrist straps, and use standard antistatic precautions.

Reseating the mission card and TM

Step	Action

At the OAMP workstation

1 Click **Configuration>platform>node**.

2 Click the icon for the system node.

3 Click **Lock** on the system node Provisioning and Maintenance window.

4 Click **Offline**.

ATTENTION
Before you unseat the CC mission card, unseat its corresponding OC-3 TM.

At the USP chassis

5 Before you unseat the TM, remove the connector(s) attached to it by unscrewing the thumbscrews on the top and bottom of each connector. Gently pull off the cable connector(s) for the TM.

6 Press outward on the top and bottom latches of the mission card or TM to release it from the CAM shelf. Two audible clicks can be heard when the mission card or TM is released completely.

7 Grasp the top and bottom latches of the mission card or TM and gently pull it toward you to remove it from the CAM shelf.

8 Ensure the top and bottom latches are in the outward position by pressing outward on each latch.

9 Position the top and bottom latches facing you, and gently slide the mission card or TM into the card guide of the one you removed, seating the bottom of the mission card or TM into the card guide and then the top.

10 Apply pressure to the faceplate until you feel resistance.

11 Snap the top and bottom latches of the mission card or TM inward, toward one another. Two audible clicks can be heard when the mission card or TM is seated properly.

12 After you reseat the TM, plug in its TM connector(s) and turn the thumbscrews on the top and bottom of the connector(s) to tighten.

13 On the front and rear of the CAM shelf, press the Lamp Test buttons. If the LEDs do not light for the system node, replace the mission card and/or TM, as described in "Replacing the mission card and TM" (page 204).

—End—

CAUTION
Wear wrist straps, and use standard antistatic precautions.

Replacing the mission card and TM

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the icon for the system node.
3	Click **Lock**.
4	Click **Offline**.
	At the USP chassis
5	Obtain a new mission card and TM, verify they have the correct PEC labels, and ensure the top and bottom latches are in the outward position.

ATTENTION
Before you replace a CC mission card, unseat its corresponding OC-3 TM.

6	Complete steps 5 to 8 from "Reseating the mission card and TM" (page 202).
7	Position the top and bottom latches of the new mission card or TM facing you, and gently slide the mission card or TM into the card guide of the one you removed, seating the bottom of the mission card or TM into the card guide and then the top.
8	Apply pressure to the faceplate until you feel resistance.
9	Snap the top and bottom latches of the mission card or TM inward, toward one another. Two audible clicks can be heard when the mission card or TM is seated properly.
10	After you reseat the TM, plug in its TM connector(s) and turn the thumbscrews on the top and bottom of the connector(s) to tighten.

11 On the front and rear of the CAM shelf, press the Lamp Test buttons. If the LEDs do not light for the system node you just replaced, ensure the mission card and TM are seated properly by unseating each and completing steps 6 to 11 again.

12 If the LEDs light, on the system node Provisioning and Maintenance window, click **Load** and wait for the system node to enable.

13 Click Unlock to ensure the system node returns to full service.

14 If the system node does not enable, contact your next level of support.

—End—

Recover a CC system node

To recover a CC system node, complete the following procedures as, as required:

- Load the CC system node, see "Loading the CC system node" (page 205).
- Reseat the mission card and TM, see "Reseating the mission card and TM" (page 202).
- Replace the mission card and TM, "Replacing the mission card and TM" (page 204).

Loading the CC system node

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the appropriate CAM shelf icon.
3	Click the icon for the system node.
4	Click **Lock** if the CC system node is not locked.
5	Click **Load** and wait for the CC system node to enable.
6	Click **Unlock** to ensure the system node returns to full service.
7	If the CC system node does not return to full service, reseat the mission card and TM of the CC system node, as described in "Reseating the mission card and TM" (page 202).

—End—

SCCP Management, 13: LSS Alarm (Critical, Major, Minor)

Description

ATTENTION
This alarm is common to Signaling Gateway, Number Portability and Service Location Register applications. For more generic information on this alarm please see the Fault section of the USP OUFCAPS suite.

This alarm occurs when the number of local subsystem (LSS) instances is not sufficient. The severity of the alarm is indicated as follows:

- Critical -- There are no LSS instances in the allowed or congested state. This usually indicates that all NPC and NPS cards have either failed or become disconnected from the system.
- Major -- There is only one LSS instance in the allowed or congested state and the minimum required number of LSS instances is at least two.
- Minor --The number of LSS instances in the allowed or congested state falls below the provisioned minimum required value.

Corrective action

Make sure there is a sufficient number of LSS instances activated. To activate an LSS, complete the following procedure.

CAUTION
Activating an NP LSS instance affects all LSSs associated with that instance.

Activating an LSS instance

Step	Action
	At the OAMP
1	Click **Configuration>np>lss**.
2	Click the **LSS Instances** button to open the Local Subsystem Instances window.
3	Locate the NP LSS instance that you want to activate. All NP LSS instances are listed in the LSS Instance Records field, at the bottom of the window. Scroll through the list to find the LSS instance you want to activate. Click the LSS instance to select it.

4 In the LSS Instance Status portion of the window, click **Activate**.

You can click Activate All to activate all provisioned NP LSS instances.

5 Click **Apply**.

—End—

TXMGR GROUP, TXMGR TCB MEMORY LOW (Minor)

Description

The memory resources allocated for managing TCAP conversations are getting low.

TCAP conversations are used for calls that require overlapped outpulsing or NPE expansion card are in use. A depletion of the transaction manager transaction control block memory (TXMGR_TCB_MEMORY) is caused by a sustained high rate of query traffic that requires overlapped outpulsing or NPE expansion card are in use.

Corrective action

No user action is required. The alarm condition will clear automatically. If the alarm condition persists or worsens, the system generates a major alarm.

TXMGR GROUP, TXMGR NO TCB MEMORY (Major)

Description

The memory resources allocated for managing TCAP conversations are getting very low.

An NP local subsystem (LSS) instance is receiving more overlapped outpulsing queries than it can handle, or NPE expansion card are in use.

The system invokes LSS instance congestion controls. The system does not allow to open new transactions on the affected NP LSS instance. New transactions are redirected to other NP LSS instances.

Existing transactions are allowed to complete on the affected NP LSS instance. Eventually, sufficient memory resources will be recovered and the alarm will clear. However, it is possible that the amount of diverted messages will become high enough to affect other NP LSS instances and eventually could cause the entire local subsystem to become congested.

Corrective action

Analyze the amount of overlapped outpulsing traffic being sent to each NP LSS and make adjustments to the traffic distribution to alleviate the overloading of the NP LSS instances before the entire LSS becomes congested.

REX Alarms

System Node Maintenance, 65: REx did not complete (Major)

Description

This alarm is raised when an RTC Routine Exercise Test has been aborted for one of the following reasons:

- user request
- mated nodes are not unlocked and enabled
- a critical alarm is unresolved
- unexpected RTC state change may have occurred (i.e. by another user)
- alternate boot audit did not pass (this test is performed at the start of the rex cycle only)
- a CLI bulk input is in progress

Corrective action

This alarm may indicates that REX aborted while one of the RTCs was locked. The state of RTC 12 and 15 needs to be verified and the RTC must be recovered (if required). If both RTCs are in-service then no action is required.

This alarm will clear on the next Successful REX cycle (either the next scheduled REX or a manually initiated REX cycle).

Recover an RTC

To recover an RTC, complete the procedure "Reloading the affected RTC system node" (page 166).

Carrier VoIP

USP Fault Management

Publication: NN10071-911
Document status: Standard
Document version: 08.02
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.