



Call Agent Fault Management

This document describes fault management strategies for diagnosing and resolving faults on the Call Agent. This document also provides references to other fault management documents for diagnosing faults on other equipment in the CS 2000 - Compact.

What's new in fault management for SN08

The following procedures are added:

- [Replacing a BIP alarm module](#)
- [Removing a BIP alarm module](#)
- [Installing a BIP alarm module](#)

The following logs support the Geographic Survivability:

- CCA685 (new) indicates that CCA *disabled* OSPF on the local Ethernet Routing Switch 8600.
- CCA686 (new) indicates that CCA *enabled* OSPF on the local Ethernet Routing Switch 8600.
- CCA331, CCA335 and CCA336 (changed) provide enhanced descriptions of monitored connection states. Associated information logs CCA631, CCA635 and CCA636 contain the descriptions. These descriptions are included only when Geographic Survivability is enabled.

When the feature is enabled, the alarm severity descriptions for [CON](#), [MatCon](#), [CON NetCon](#) and [CON LnkCon](#) include the same enhanced descriptions.

For details and examples of these logs, refer to *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909.

The severity of the following alarms have been changed to support Geographic Survivability:

- [CON MatCon](#): previously minor and major alarms are now major and critical alarms, respectively
- [CON NetCon](#): previously major and critical alarms are now minor and major alarms, respectively

Prior to SN08, the Card View panels for the SAM21manager GUI and Gateway Controller (GWC) manager GUI both had the label “Administrative.” In the GWC manager, the label indicated the state of an application running on a card. However, in the SAM21 manager, the label indicated the hardware state of a card.

To eliminate confusion, in SN08 the label “Administrative” has been changed to “Card Status” in every card view of the SAM21 manager GUI.

Contents

| | |
|--|------------|
| Call Agent Fault Management | 1 |
| What's new in fault management for SN08 | 1 |
| Network fault management strategy | 5 |
| Replacing a Call Agent card | 20 |
| Replacing a Call Agent Transition Module | 29 |
| Perform a maintenance switch of activity on a Call Agent | 40 |
| Returning a Call Agent card to Nortel | 45 |
| Replacing a BIP alarm module | 46 |
| Removing a BIP alarm module | 48 |
| Installing a BIP alarm module | 50 |
| Replacing cooling unit fan filters | 53 |
| Testing wrist-strap grounding cords | 58 |
| | |
| Call Agent Manager alarm clearing procedures | 60 |
| Additional information | 61 |
| Retrieving logs | 63 |
| Call Agent alarm and log matrix | 66 |
| CallAgent Jlnact | 69 |
| CallAgent RExFlt | 70 |
| CallAgent RExTst | 73 |
| Call Agent RExSch | 74 |
| CallAgent simplx | 76 |
| CallAgent C_MisM | 78 |
| Call Agent Config | 79 |
| CallAgent NIIKEY | 80 |
| SYS CPU Ld | 81 |
| SYS Disk | 83 |
| SYS Memory | 84 |
| SYS NFS | 86 |
| SYS NTP | 89 |
| SYS Zombie | 92 |
| SYS CpuUtl | 93 |
| SYS HW Flt | 95 |
| CON MatCon | 96 |
| CON LnkCon | 100 |
| CON NetCon | 103 |
| APPL NoAppl | 106 |
| APPL ImgTst | 107 |
| APPL Image | 108 |
| APPL simplx | 110 |
| APPL Memory | 112 |
| | |
| MAP alarm clearing procedures | 113 |
| MTC level | 113 |
| APPL alarms | 115 |
| IOD ITOC | 116 |

IOD DISK 120
Creating a test volume on a disk 124
Recording an office image on a disk 127
Restoring a Call Agent 137
Copying files from disk to tape 140
Backing up files to DVD-RW 146
Restoring files from a DVD-RW 156
Scheduling automatic image taking 160
How to change REx Tst (routine exercise test) intensity 168

CS 2000 SAM21 Manager procedures **169**

Card icons 170
Running diagnostics 175
Monitoring diagnostics 177
Aborting diagnostics 178
Retrieving alarms 179

Message controller procedures **185**

Fault management strategy 185
Connectivity 186
Viewing Message Controller status 189
Running diagnostics 201
MC ATM 209
MC ETH 214
MC MCTbl 217

Network fault management strategy

Faults on the Call Agent and the call processing application generate alarms and logs. Hardware and software platform alarms are accessible through the Call Agent Manager. Call processing alarms are accessible through the MAP. Logs for the platform are available through the Call Agent Manager. Logs for the call processing application are available through the MAP. Both types of logs are also transferred to the CS 2000 Core Manager or CBM for Operations Support System (OSS) transfer.

In the event of a platform software error that prevents the Call Agent from providing service, software attempts to automatically restore service. In this event, the Call Agent Manager immediately indicates the mate failure. A periodic shelf audit by the SAM21 Shelf Controller reports the Call Agent state to the CS 2000 SAM21 Manager when the audit runs. If the Call Agent has a platform failure, the CS 2000 SAM21 Manager indicates that the Call Agent state is unlocked-enabled but the software on the card is actually disabled. The Call Agent card enters an automatic recovery sequence to restore service. The automatic recovery has two stages:

1. Motorola firmware on the card performs a Network Autoboot
2. If the Network Autoboot fails and does not restore service, the SAM21 Shelf Controller performs an autoboot on the Call Agent card.

As the Call Agent card recovers, the SAM21 Shelf Controller generates SM21500 log reports during each state transition. Refer to *SAM21 Shelf Controller Fault Management*, NN10089-911 for more information about the recovery. Refer to [Card icons](#) for information about card icons and states at the CS 2000 SAM21 Manager client.

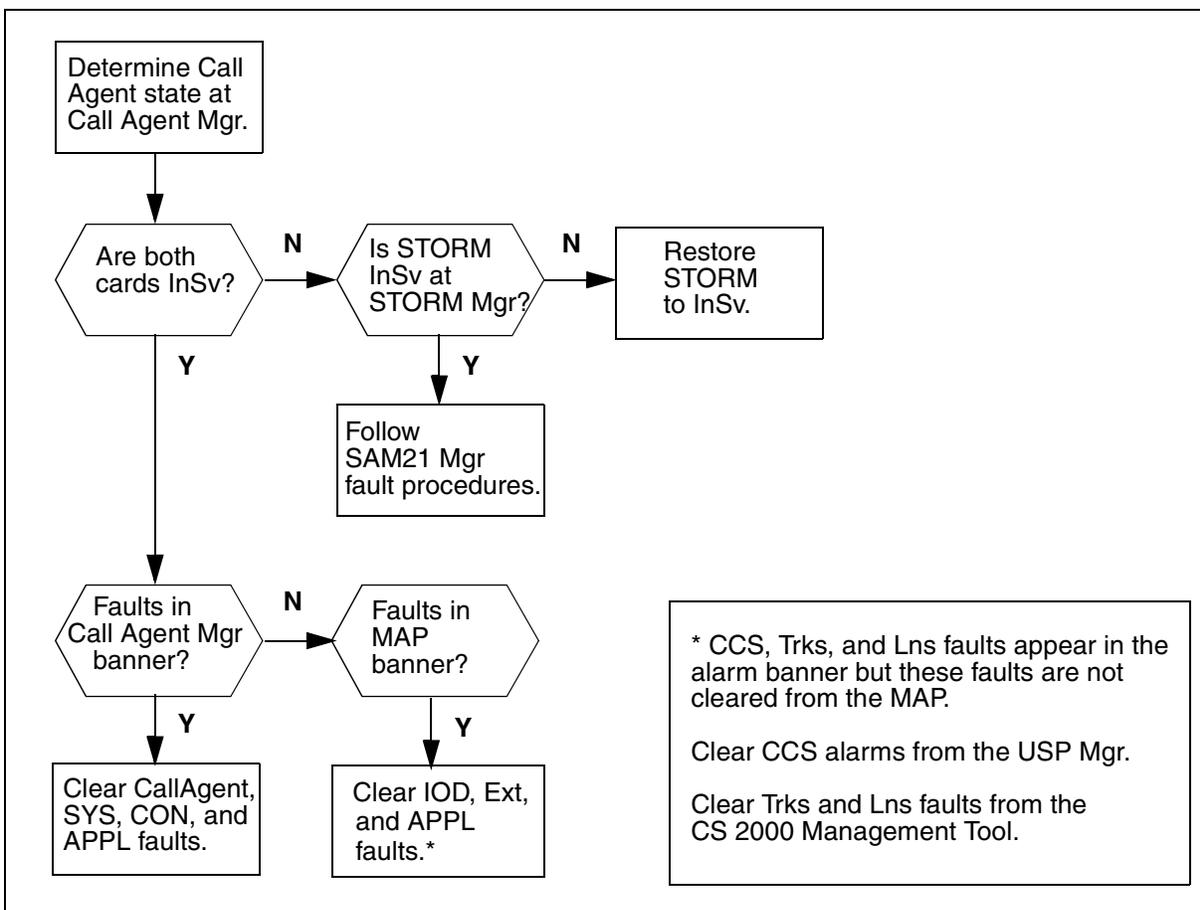
In the event that Ethernet connectivity between the Call Agent cards is lost, activity is switched to the Call Agent with Ethernet connectivity and the inactive Call Agent is reset. Loss of Ethernet connectivity can be caused by an Ethernet link pull, router misconfiguration, or a router problem. Refer to the following table for the conditions and reset

method. If the backup link (BLnk) is available, it is used to message the activity change request and the reset request.

| Call Agent activity | BLnk state | Reset method |
|---------------------|------------|--|
| Active | InSv | The active Call Agent has lost Ethernet connectivity and uses the BLnk to switch activity (SWACT). The newly inactive issues a reset request to the newly active and starts a 60 second reset timer. The active accepts the request and starts a 20 second reset timer. After 20 seconds, the active sends a reset request to the inactive Call Agent's SAM21 Shelf Controller. If the reset does not occur before the inactive's 60 second timer, the inactive resets itself. |
| Active | OOS | A SWACT takes place and the newly inactive Call Agent resets itself in 130 seconds. |
| Inactive | InSv | Activity does not switch and the inactive Call Agent starts a 60 second reset timer. The inactive sends a reset request message over the BLnk to the active. The active accepts the request and starts a 20 second timer. When the 20 second timer expires, the active sends a reset request to the inactive's SAM21 Shelf Controller. If the SAM21 Shelf Controller does not reset the inactive within the 60 second timer, the inactive resets itself. |
| Inactive | OOS | The inactive sets a 60 second reset timer and resets itself when the timer expires. |

Fault management taskflow

Use the following flowchart as a guideline to diagnosing a fault and locating trouble clearing procedures.



- Determine the state of the Call Agent with Call Agent Manager. Refer to procedure [Call Agent Manager alarm clearing procedures on page 60](#).
- Determine if STORM is in service at the STORM Manager. If the STORM unit is based on STORM cPCI, refer to procedure [CS 2000 SAM21 Manager procedures on page 169](#). If the STORM unit is based on the SAM-XTS hardware platform (STORM-IA), refer to *STORM Fault Management*, NN10088-911.
- Determine if there are faults in the Call Agent Manager alarm banner.

Refer to procedure [Call Agent Manager alarm clearing procedures on page 60](#).

- Determine if there are faults in the MAP alarm banner.

Refer to procedure [MAP alarm clearing procedures on page 113](#).

Fault management tools and utilities

The following tools are used to manage faults on the Call Agent:

- CS 2000 SAM21 Manager client

If the Call Agent does not boot, the CS 2000 SAM21 Manager client is used as a diagnostic tool.

- Call Agent Manager

Platform faults such as simplex operation, Central Processing Unit (CPU) and memory threshold crossing, connectivity, and call processing application synchronization are reported to this interface.

- MAP

Call processing and billing faults are reported to this interface.

This document is structured so that all procedures available at each interface are grouped together. Use the following taskflow to begin diagnosing faults and follow links and references to specific procedures.

Tools, utilities, and interfaces

Fault management for the Call Agent is completed through three interfaces. The MAP is the interface to the call processing application and is command line and console oriented. Once the MAPCI command is entered at the MAP command prompt, the interface remains console oriented, but is navigated by menu commands.

MAP at the CI level

```
2003/04/03 10:48 <office message>
CI:
>
```

MAP at the MAPCI level

```
MAPCI          MAPCI :
 0 Quit
 2 Mtc
 3 SASelect
 4 NWM
 5 CPSys
 6 IBNMEAS
 7
 8 FPE
 9 TESTTOOL
10
11
12
13
14
15
16
17
18
  username
Time 14:49 >
```

The second interface is the Call Agent Manager. This interface is console oriented and is navigated by menu commands. The Call Agent Manager provides access to the hardware and software platform when

the software is in-service. The current menu level is displayed in the circled area in the figure below.

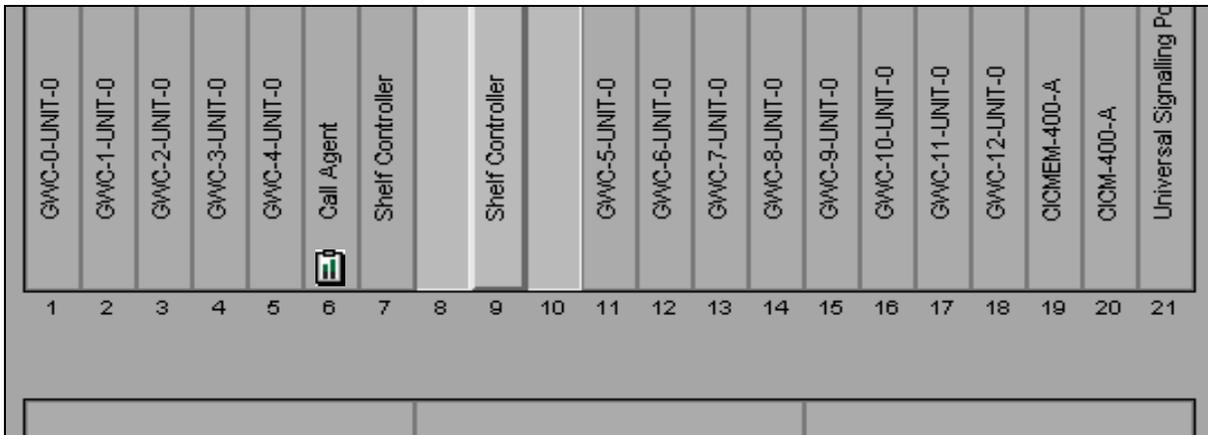
Call Agent Manager

```

CallAgent      SYS      CON      APPL      Unit: 0
.              .              .              .
CCAMtc
0 Quit
2 CoreMtc
3 Admin
4
5
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
   mtc
Time 17:10 >
    
```

The third interface is the CS 2000 SAM21 Manager. This graphical user interface (GUI) is used to perform out of service maintenance on the Call Agent hardware platform.

CS 2000 SAM21 Manager



Geographic Survivability

The Geographic Survivability feature allows services to continue in the event of a natural or man-made disaster, and enhances continued service support during normal operations. A new sub-panel is added to the Call Agent Card View Provisioning panel (tab) that allows you to either enable or disable the feature. The following figure shows an example configuration with Geographic Survivability enabled.

Call Agent Card View Provisioning panel: Geographic Survivability enabled

The screenshot displays the 'OTT4 CA-1 : Slot 6' provisioning interface. The 'Provisioning' tab is selected and circled. The 'General' section contains fields for IP (10.72.17.22), Subnet Mask (255.255.240.0), MAC Address (0001AF12AFA0), Gateway IP (10.72.16.1), FW Version (RM03-2.4), and MAC 2 (0001AF12AF9F). The 'NTP' section shows Primary NTP (47.135.43.193) and Secondary NTP (47.135.43.196). The 'Load Info' section includes Server IP (47.135.43.193), Path (/3pc), Load (ncgl_cca_image_7.02.1.0), and a 'Get Load Files' button. A 'FW Flash Enable' checkbox is checked. The 'Geographical Survivable' section is highlighted with a thick black border and contains a 'Geographical CS 2000 Compact' section with an 'Enable' checkbox checked. Below this is a 'Backup Path' section with fields for GEO UNIT 0 IP (10.72.0.12) and Mask (255.255.255.248), and GEO UNIT 1 IP (10.72.0.20) and Mask (255.255.255.248). At the bottom are buttons for 'Modify', 'Save', 'Clear', 'Cancel', 'Details...', and 'Help'.

| Field | Value |
|------------------------------|--|
| IP | 10.72.17.22 |
| Subnet Mask | 255.255.240.0 |
| MAC Address | 0001AF12AFA0 |
| Gateway IP | 10.72.16.1 |
| FW Version | RM03-2.4 |
| MAC 2 | 0001AF12AF9F |
| Primary NTP | 47.135.43.193 |
| Secondary NTP | 47.135.43.196 |
| Server IP | 47.135.43.193 |
| Path | /3pc |
| Load | ncgl_cca_image_7.02.1.0 |
| FW Flash Enable | <input checked="" type="checkbox"/> |
| Geographical CS 2000 Compact | <input checked="" type="checkbox"/> Enable |
| GEO UNIT 0 IP | 10.72.0.12 |
| Mask | 255.255.255.248 |
| GEO UNIT 1 IP | 10.72.0.20 |
| Mask | 255.255.255.248 |

Failure scenarios

The following table provides summaries of system responses during various failure scenarios when Geographic Survivability is enabled. The scenarios assume redundant configurations are located in two separate buildings.

System response summaries

| Scenario | Response |
|---|--|
| Ethernet Routing Switch 8600 failure in one building | <p><i>In the building with the failed routing switch...</i></p> <ul style="list-style-type: none"> • All nodes lose mate connectivity via Ethernet. • The Call Agent loses WAN backup connectivity. • FC backup remains up. • The Call Agent detects IST loss, but cannot disable OSPF. • USPc detects isolation and takes down SS7 links at the site with the 8600 failure. <p><i>In the building with the in-service routing switch...</i></p> <ul style="list-style-type: none"> • The Call Agent remains active if it is already active. No outage occurs. If the Call Agent was not active, it takes activity within 2 seconds. • SOS goes through a warm or cold restart (approximately 30 seconds). • Other nodes go active and follow the Call Agent example after losing mate connectivity. • If Building B has the in-service router, the standby CS 2000 Management Tools (CMT) server must be brought into service. (See Note) • If Building A has the in-service router, the standby Core Billing Manger (CBM) must be brought in to service. (See Note) <p>Note: Consider using this option based on the estimated time to recover the fault or failure of the CS LAN versus time and effort to bring up the standby system and recover the high availability (HA) pair afterward.</p> <p>For example, if the time to recover the CS LAN is estimated to be 10 hours, it might not be worth activating the standby CMT server or CBM.</p> |

System response summaries

| Scenario | Response |
|--|--|
| Optical frame failure in one building | <p><i>In the building with the failed optical frame...</i></p> <ul style="list-style-type: none"> • All nodes lose mate connectivity via Ethernet. • The Call Agent loses FC backup connectivity. • WAN backup remains up. • The active Call Agent remains active, but without sync. No outage occurs <i>The remainder of this scenario assumes the active Call Agent is in this building.</i> • Other nodes go active and follow the Call Agent example after losing mate connectivity. (Done without mate connectivity.) <p><i>In the building with the in-service optical frame...</i></p> <ul style="list-style-type: none"> • The Call Agent detects IST loss, and disables OSPF. • Other nodes go inactive and follow the Call Agent example after losing mate connectivity. (Done without mate connectivity.) • USPc detects isolation from the active Call Agent, and takes down SS7 links at the site with the inactive USP. • If Building B has the failed optical frame, the standby CBM must be brought into service at Building A. (See Note) • If Building A has the failed optical frame, the standby CMT must be brought into service at Building B. (See Note) <p>Note: Consider using this option based on the estimated time to recover the fault or failure of the optical frame versus time and effort to bring up the standby system and recover the high availability (HA) pair afterward.</p> <p>For example, if the time to recover the optical frame is estimated to be 10 hours, it might not be worth activating the standby CMT server or CBM.</p> |

System response summaries

| Scenario | Response |
|--|--|
| One building is destroyed in a catastrophic event | <p data-bbox="570 359 1081 394"><i>In the building that is destroyed...</i></p> <ul data-bbox="570 407 1411 520" style="list-style-type: none"><li data-bbox="570 407 889 443">• There is no activity.<li data-bbox="570 455 1411 520">• The SS7 network takes down the links to the destroyed building. <p data-bbox="570 533 1138 569"><i>In the building that is not destroyed...</i></p> <ul data-bbox="570 581 1411 1129" style="list-style-type: none"><li data-bbox="570 581 1081 617">• All nodes lose mate connectivity.<li data-bbox="570 630 1411 695">• The Call Agent loses all mate connectivity, backups and sync.<li data-bbox="570 707 1411 800">• The Call Agent remains active if it is already active. No outage occurs. If the Call Agent is not active, it takes activity within 2 seconds.<li data-bbox="570 812 1411 884">• SOS goes through a warm or cold restart (approximately 30 seconds).<li data-bbox="570 896 1411 968">• Other nodes go active, and follow the Call Agent example after losing mate connectivity.<li data-bbox="570 980 1411 1045">• If Building B was destroyed, the standby CBM must be brought into service at Building A.<li data-bbox="570 1058 1411 1129">• If Building A was destroyed, the standby CMT must be brought into service at Building B. |

System response summaries

| Scenario | Response |
|--|---|
| Active Call Agent card fails in one building | <p><i>In the building with the failed Call Agent...</i></p> <ul style="list-style-type: none"> All nodes in the site can communicate with their mates. <p><i>In the building with the mate Call Agent...</i></p> <ul style="list-style-type: none"> All nodes in the site can communicate with their mates. The (inactive) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, takes activity, and restarts the SOS. Other nodes experience disconnection from the SOS for approximately 30 seconds (normal restart behavior). |
| Inactive Call Agent card fails in one building | <p><i>In the building with the failed inactive Call Agent...</i></p> <ul style="list-style-type: none"> All nodes in the site can communicate with their mates. <p><i>In the building with the mate Call Agent...</i></p> <ul style="list-style-type: none"> All nodes in the site can communicate with their mates. The (active) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, and stays active. No SWACT or restart is required. |
| Recovery from isolation split brain (Active/Inactive) | <p><i>In both buildings...</i></p> <ul style="list-style-type: none"> Once the Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active and Unit 1 inactive. Other nodes can communicate with their mates, negotiate activity, and resume normal operations. |

System impact of failures

Failures could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to remain on the same side, if that side supports activity.
- If failover of the Call Agent is necessary, the Call Agent switches activity in less than two seconds. When the Callp Application performs a restart, call processing is interrupted for approximately 30 seconds. Failovers of other Callp nodes follow the Call Agent failover within two seconds.
- In configurations where the solution contains Message Controller (MC) cards connected to Message Switches (MS), ENET and TDM peripherals, the MC cards and MSes are co-located in one of the main geographically redundant sites.

During building isolation, when determining the appropriate master site, preference is given to the site that contains the MC cards. This assumes that the site is able to take activity. If necessary, activity is switched to this side during the activity negotiation.

This configuration is supported only in Enterprise (CS2100) solutions.

Recovery scenarios

The following table provides a summary of system responses during recovery.

System response summary

| Scenario | Response |
|--|--|
| Recovery from isolation split brain (Active/Inactive) | <ol style="list-style-type: none"> 1. When Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive before the failure backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active, and Unit 1 inactive. 2. Other nodes can communicate with their mates, negotiate activity and resume normal operations. |
| General recovery behavior | <p>All elements:</p> <ul style="list-style-type: none"> • continually monitor connections with their mates, and with other network elements with which they normally communicate. When connectivity is not present, they continue to monitor the connections for restored connectivity. (The elements continue monitoring regardless of their activity state.) • negotiate activity and services when connectivity recovers, and resume normal operations. |

System impact of recovery

Recovery could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to leave activity on the same side. When recovering to a full system configuration, activity remains on the same unit, without impact.
- During recovery from a split system (caused by incorrect message routing), node activity resolves in a few seconds. Call processing could require up to 15 minutes to recover completely.

Limitations and restrictions

Please note the following restrictions for the Geographic Survivability feature:

- In hybrid configurations (with TDM equipment homed at one site), the TDM equipment is not geographically redundant. In determining the master site, preference is given to the TDM side only when either side can support Callp. If necessary, a SWACT is performed to the TDM side to allow Callp on that side.

This configuration is supported on in Enterprise (CS2100) solutions.

- Because the Call Agent must interact with the Ethernet Routing Switch 8600, the feature requires that each site have only one routing switch and IST links configured between sites. Dual 8600's at each site and SMLT links between sites are not supported. Only 8600 routing switches are supported. Upgrades from previous releases in the geographically redundant configurations (which have dual 8600's at each site) require that the dual 8600's be migrated to a single PP8600 site.
- When a total loss of communication between sites occurs (that is, all three master links are down), the two Call Agents cannot negotiate activity decision. The decision is based on connectivity check from each site the WAN network.
 - While unlikely, it could be possible to have an active/active (split brain) scenario, or an inactive/inactive scenario (no processing).
 - The WAN backup path mitigates the risk of optical ring failure. The WAN connection check helps resolve activity when the backup path is down.
- CS 2000 - Compact supports only a single time zone setting. If the two physical sites are in different time zones, it recommended that the time zone be set to either GMT or the time zone of one of the sites.
- Both NGSS units are home on one site. For offices with message controllers (CS2100), it is recommended that the NGSS be homed on the same site as the TDM components.
- For maximum redundancy, the WAN backup path must be configured separately from the optical network, as follows:
 - special vlans configured on Ethernet Routing Switch 8600 for backup path use only
 - vlans route over the WAN network instead of over the optical ring

- vlans are not disabled with OSPF disable
- alarm generated for lack of connectivity
- Gateways and services node components of CS 2000 - Compact are single units, and are not geographically redundant. Where the nodes are located and how they are connected to the network affects whether they survive a failure. Although the same nodes are supported in configurations with and without Geographic Survivability, there is no change in configuration or connection in the configuration with the Geographic Survivability configuration.

For more information about the feature, refer to the following documents:

- *Call Agent Basics*, NN100223-111
- *Carrier VoIP Disaster Recovery Procedures*, NN10450-900

For offices configured with Message Controllers, refer to *Geographic Survivability Planning Guide*, 555-4031-901.

Note: Configurations with MCs are supported only in Enterprise (CS2100) solutions.

For more information about alarm and log changes and system behavior during fault scenarios for Geographic Survivability, refer to *Call Agent Fault Management*, NN10087-911.

Replacing a Call Agent card

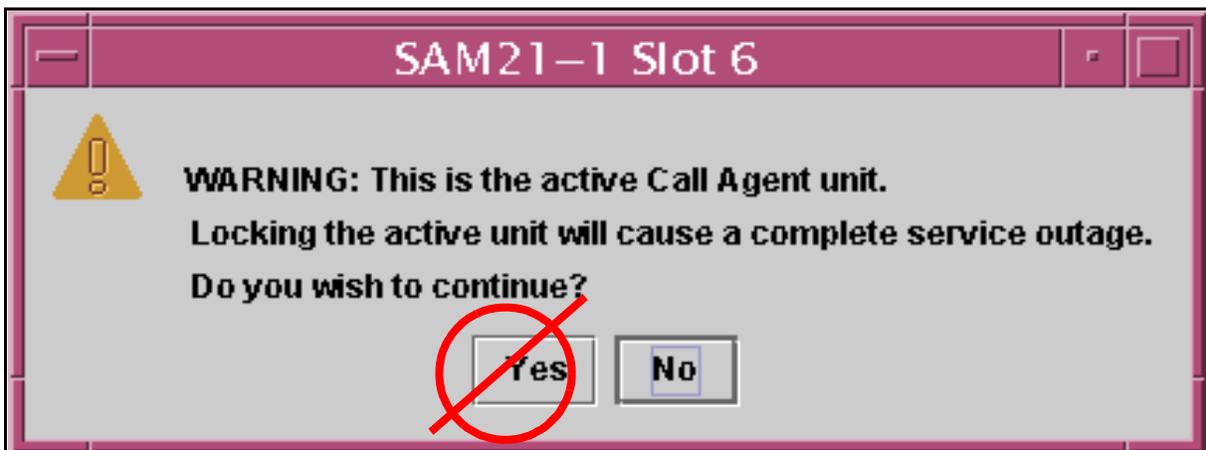
**CAUTION****Possible service interruption**

Perform this procedure at the direction of Nortel support personnel.

**CAUTION****Possible service interruption**

Do not lock the active Call Agent.

The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the following prompt. Do not click Yes.



Note: This warning message appears for both Call Agent units for a short time after both units are brought into service. After unlocking a Call Agent card, wait 15 minutes before requesting a lock on either Call Agent.

At the Call Agent Manager

- 1 If the Call Agent to be replaced is in service and active, DpSync from the Call Agent Manager, then SWACT the call processing application in the BCSUPDATE level of the MAP with commands LIMITED_PRESWACT, and NORESTARTSWACT. If DpSync is used here, don't use it in [step 3](#).
- 2 Jam the inactive Call Agent from the CAMtc level.

CoreMtc**CAMtc****Jam****Note:** A JInact alarm appears in the alarm banner.

```

CallAgent      SYS      CON      APPL      Unit: 0
JInact
CAMtc
0 Quit        Unit0  Act      no      . Act    . Inact  .      .      insync .
2 Jam        Unit1  Inact    yes     . Act    . Inact  .      .      insync .

```

- 3 Drop synchronization of the call processing software between the two Call Agents at the Appl level.

CoreMtc**Appl****DpSync****Note:** A simplex alarm appears in the alarm banner and the applications report nosync.

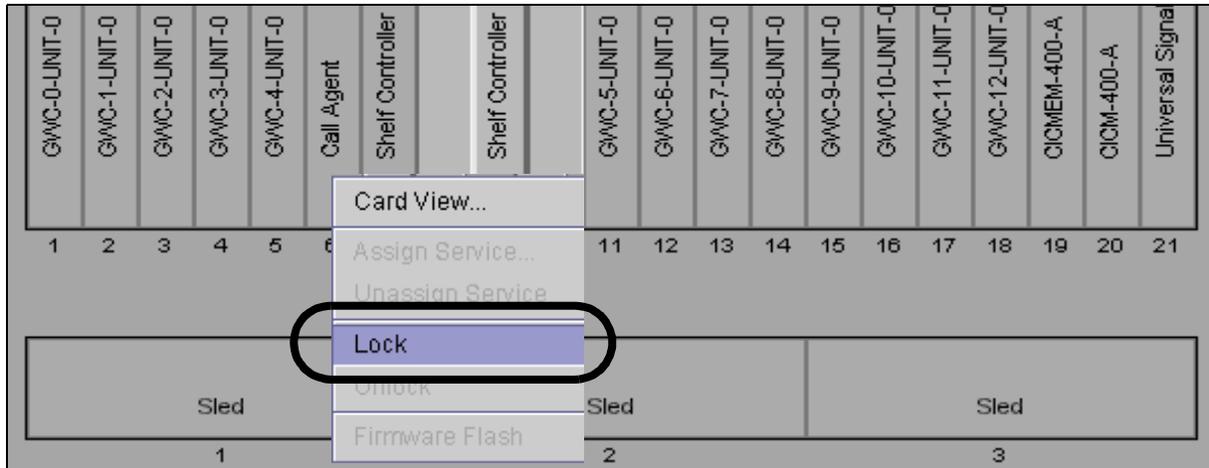
```

CallAgent      SYS      CON      APPL      Unit: 0
JInact
CAMtc
0 Quit        Unit0  Act      no      . Act    . Inact  .      .      nosync .
2 ImgTst     Unit1  Inact    yes     . Act    . Inact  .      .      nosync .

```

At the CS 2000 SAM21 Manager client workstation

- 4 From the Shelf View, right click on the card and select Lock from the context menu.



- 5 Wait for the lock icon to appear on the selected card.

At the SAM21 frame

- 6 Label and remove the fiber connection from the faceplate. Unscrew the captive screws.
- 7 Open the bottom ejector lever.

Note: Wait for the green LED on the faceplate to extinguish and a blue LED to light at the bottom of the faceplate.
- 8 Wait for the blue LED to appear at the bottom of the faceplate and the red out-of-service LED that is above the card to extinguish.
- 9 Press both ejector levers to eject the card from the shelf.
- 10

**CAUTION****Possible service interruption**

A service outage can occur if care is not taken while inserting the circuit pack.

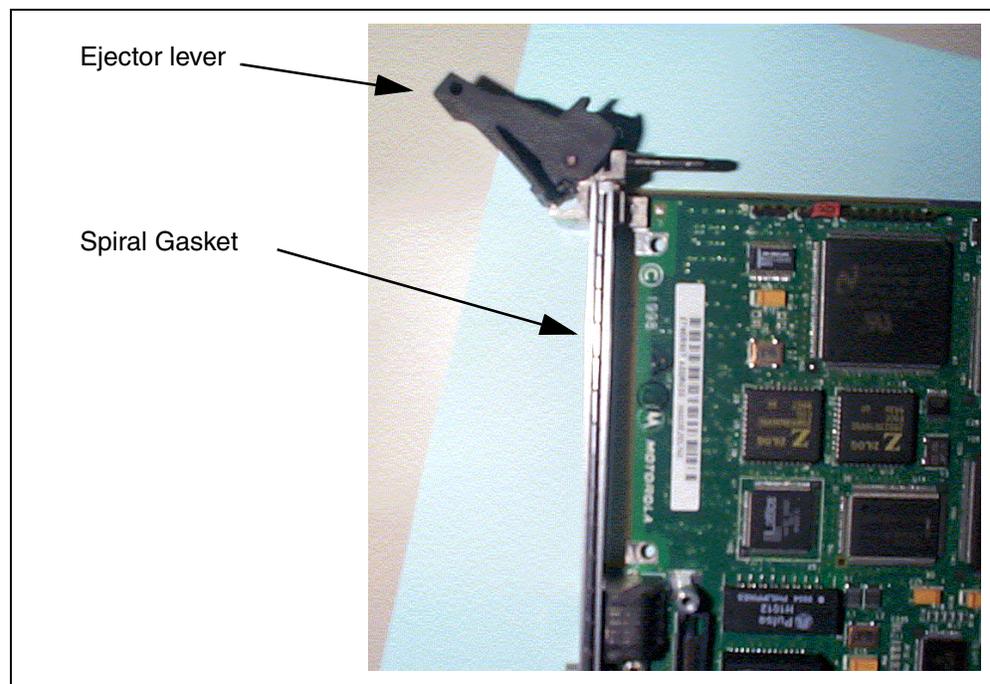
The spiral gasket, located on the faceplate of the circuit pack, can become caught on an adjacent card and ripped off of the faceplate. If the spiral gasket ends up making contact with the backplane inside the chassis, an electrical short circuit can result in a service outage.

**WARNING****Static electricity damage**

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the SAM21 Shelf Cabinet when handling the replacement card. This protects the card against damage caused by static electricity.

Hold the replacement card by the ejector levers and remove the card from the shelf.

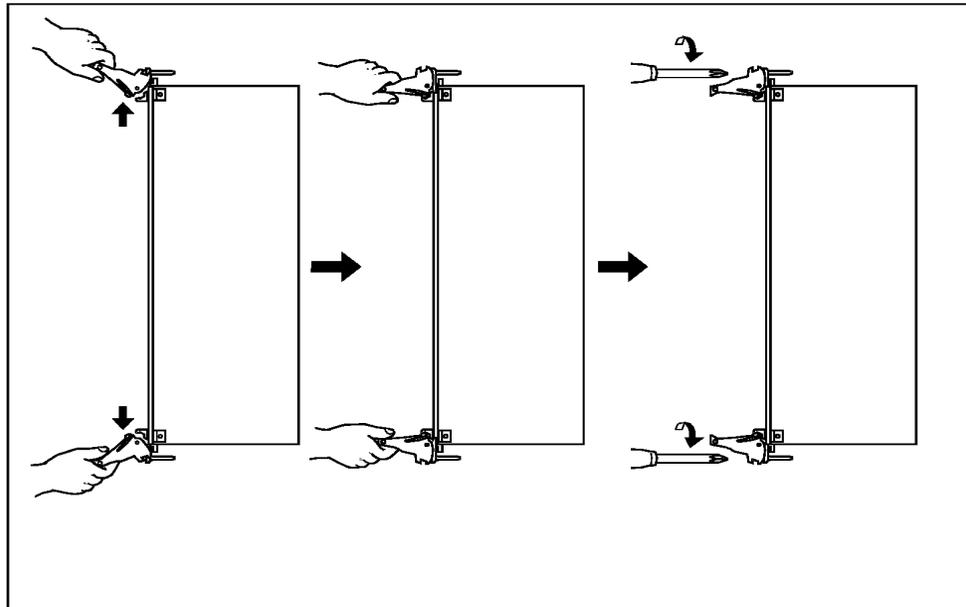
- 11 Examine the circuit packs before inserting them in the SAM21 chassis to ensure that the spiral gasket is seated and not loose.



- 12 Hold the replacement card by the ejector levers and insert the card into the shelf.

Note 1: Do not push on the faceplate to seat the card.

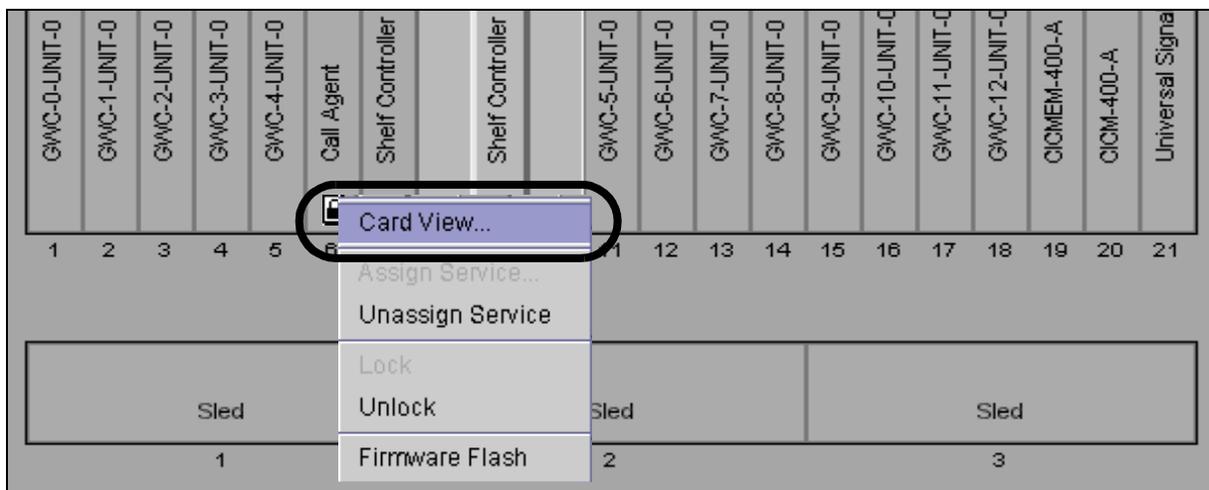
Note 2: Verify that the CPU LED lights. If the CPU LED does not light, reseal the card. If the CPU LED fails to light a second time, replace the card.



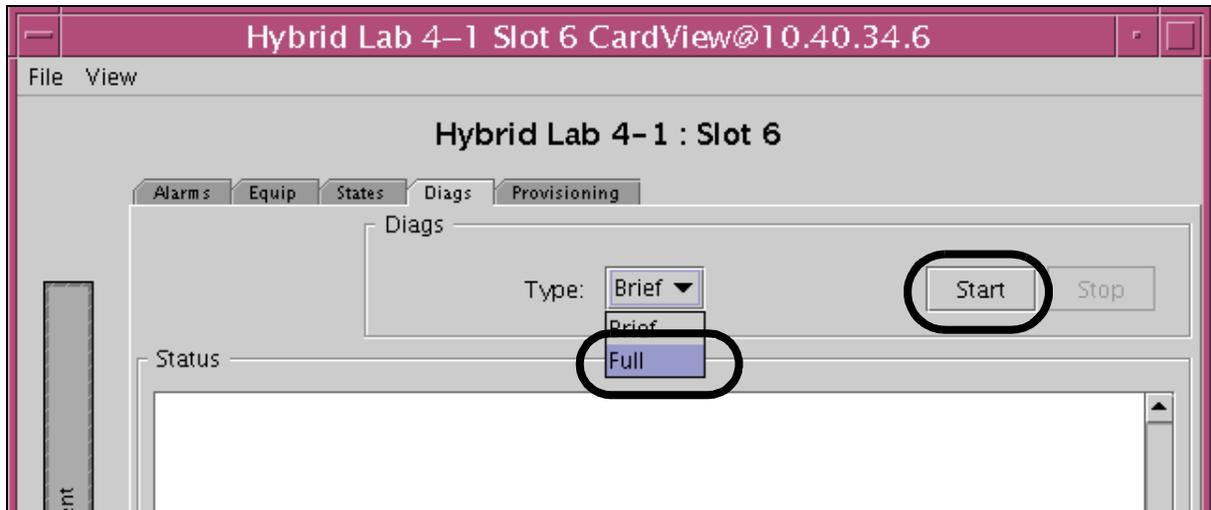
- 13 Secure the board by tightening the captive screws at the top and bottom of the panel.
- 14 Replace the fiber faceplate connections.

At the CS 2000 SAM21 Manager client workstation

- 15 Run full diagnostics on the replacement card. Right-click on the card icon in the Shelf View and select Card View from the context menu to open the Card View window.



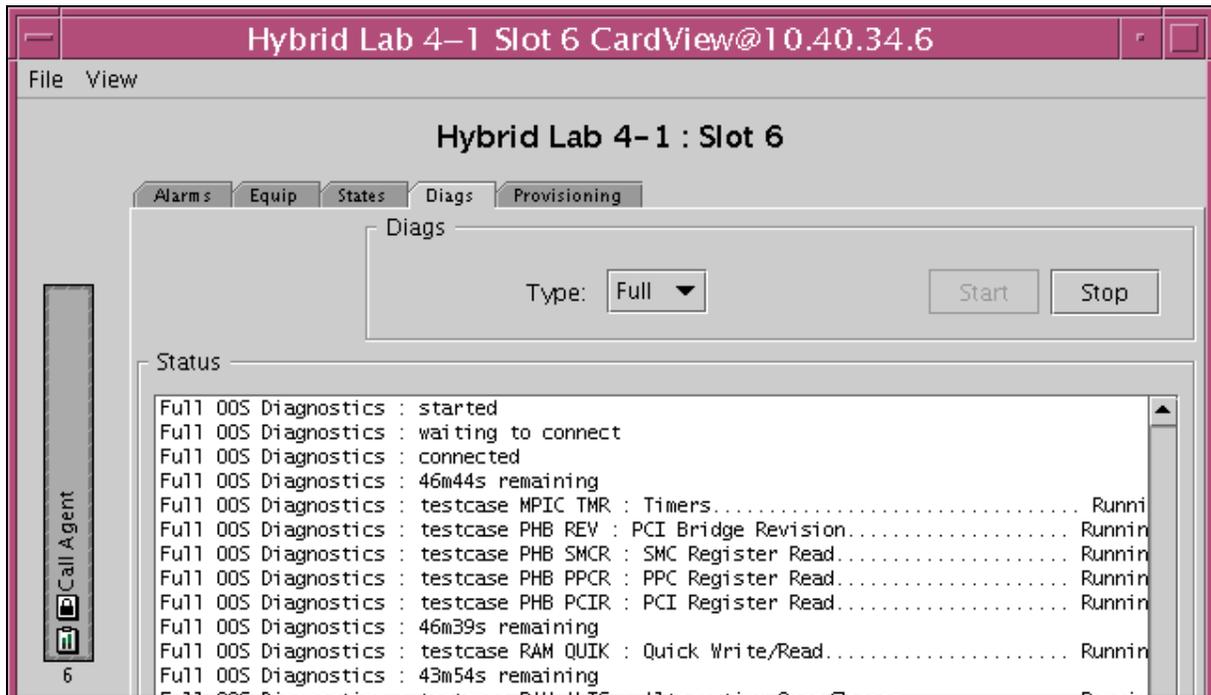
- 16** Click on the Diagnostics tab from the Card View, select Full, and then click Start.



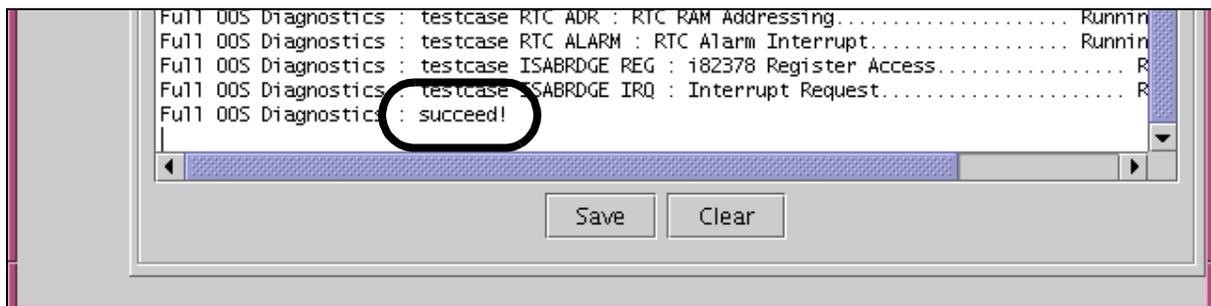
A confirmation dialog appears. Confirm the dialog.



The diagnostics begin and are printed to the Status text area.



Wait for the diagnostics to complete and verify that the last line of the diagnostic output indicates "succeed!" If diagnostics do not indicate success, retry brief diagnostics and then full diagnostics. If diagnostics fail a second time, replace the card.



20 Release the jam on the inactive unit from the CAMtc level.

CoreMtc

CAMtc

RelJam

Note: The JInact alarm clears from the alarm banner.

21 This procedure is complete.

Replacing a Call Agent Transition Module

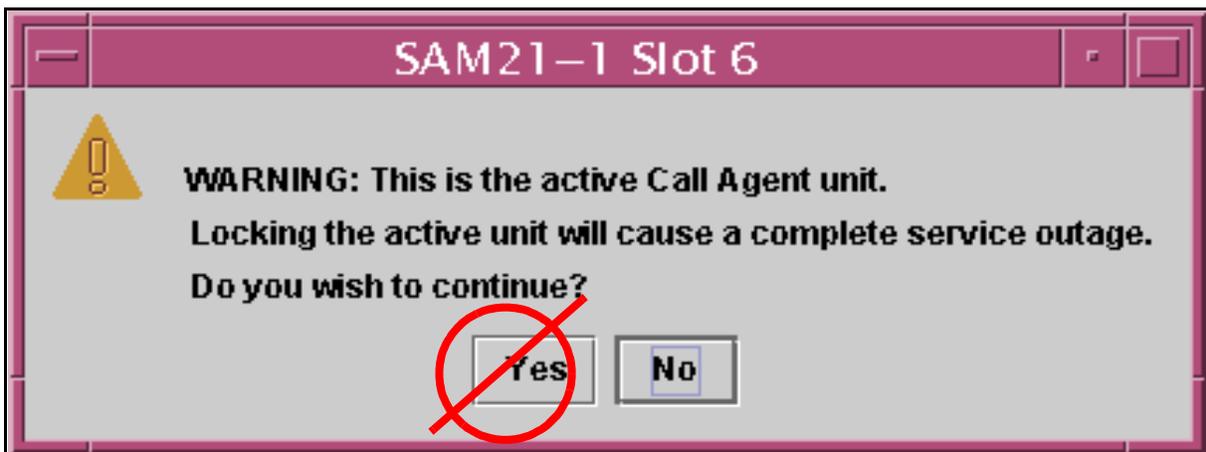
**CAUTION****Possible service interruption**

Perform this procedure at the direction of Nortel support personnel.

**CAUTION****Possible service interruption**

Do not lock the active Call Agent.

The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the following prompt. Do not click Yes.



Note: This warning message appears for both Call Agent units for a short time after both units are brought into service. After unlocking a Call Agent card, wait 15 minutes before requesting a lock on either Call Agent.

- 1 Obtain a replacement Call Agent Transition Module (TM) with PEC NTRX51FS.

At the Call Agent Manager

- 2 If the Call Agent TM to be replaced is for the Call Agent that is in service and active, DpSync from the Call Agent Manager, then SWACT the call processing application. Refer to procedure [Perform a maintenance switch of activity on a Call Agent on page 40](#).

If DpSync is used here, do not use it in [step 4](#).

- 3 Jam the inactive Call Agent from the CAMtc level.

Telnet to the active core (after bcsupdate and norestartswact, and the active core has changed), and enter your user ID and password.

```
ccamt c
CoreMtc
CAMtc
Jam
```

Note: A Jlnact alarm appears in the alarm banner.

| CallAgent | SYS | CON | APPL | Unit: 0 |
|-----------|-------|-----------|---------------|------------------------|
| Jlnact | . | . | . | |
| CAMtc | | | | |
| | | Jam: | Link0: | Link1: Blnk: FC: Appl: |
| 0 Quit | Unit0 | Act no | . Act . Inact | . . insync . |
| 2 Jam | Unit1 | Inact yes | . Act . Inact | . . insync . |

- 4 Drop synchronization of the call processing software between the two Call Agents at the Appl level.

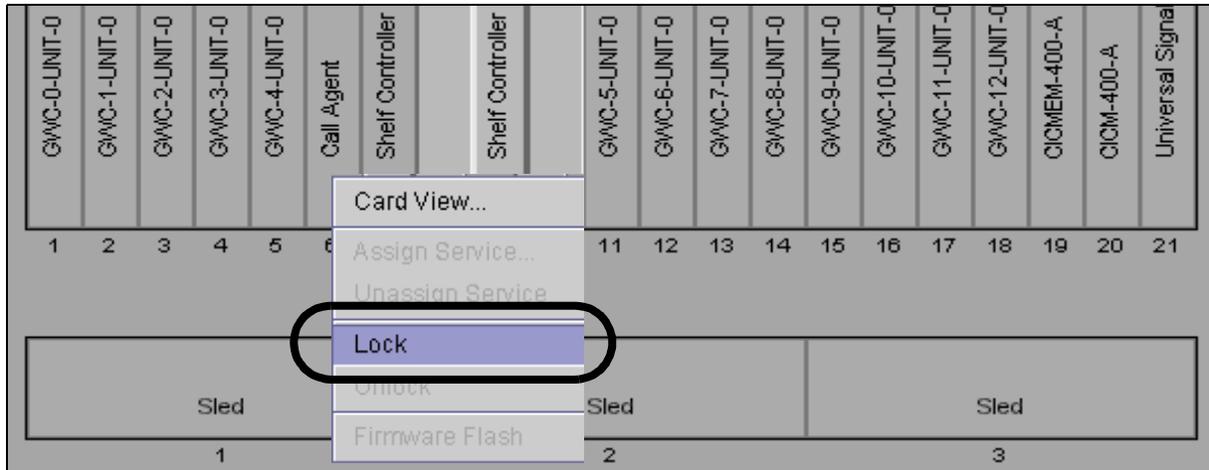
```
CoreMtc
Appl
DpSync
```

Note: A simplex alarm appears in the alarm banner and the applications report nosync.

| CallAgent | SYS | CON | APPL | Unit: 0 |
|-----------|-------|-----------|---------------|------------------------|
| Jlnact | . | . | simplex M | |
| Appl | | | | |
| | | Jam: | Link0: | Link1: BLnk: FC: Appl: |
| 0 Quit | Unit0 | Act no | . Act . Inact | . . nosync . |
| 2 ImgTst | Unit1 | Inact yes | . Act . Inact | . . nosync . |

At the CS 2000 SAM21 Manager client workstation

- 5 From the Shelf View, right click on the card and select Lock from the context menu.



- 6 Wait for the lock icon to appear on the selected card.

At the SAM21 frame

7



WARNING

Static electricity damage

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the wrist strap grounding point, which is located on the local craft access panel (LCAP), when handling cards. This protects the cards against damage caused by static electricity.

Unscrew the captive screws on the Call Agent card.

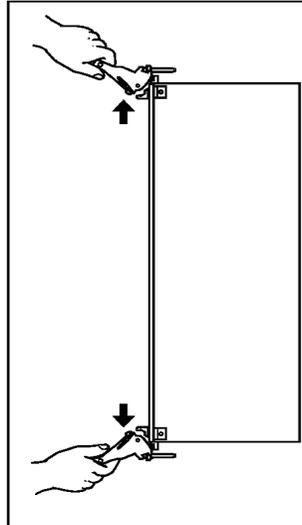
Note: Power to the Call Agent TM is removed by unseating the Call Agent card at the front.

- 8 Open the bottom ejector lever.

Note: Wait for the green LED on the faceplate to extinguish and a blue LED to light at the bottom of the faceplate.

- 9 Wait for the blue LED to appear at the bottom of the faceplate and the red out-of-service LED that is above the card to extinguish.

- 10 Push the top ejector lever up and bottom ejector lever down as shown in the figure that follows, to eject the card from the shelf, and slide the card out slightly.



At the rear of the SAM21 frame

11

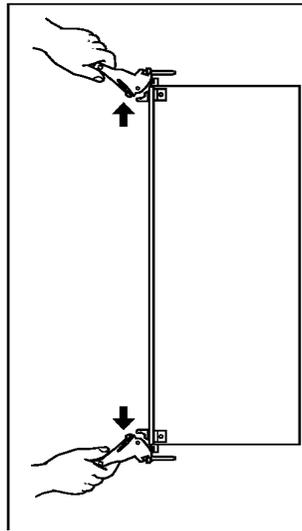


WARNING

Static electricity damage

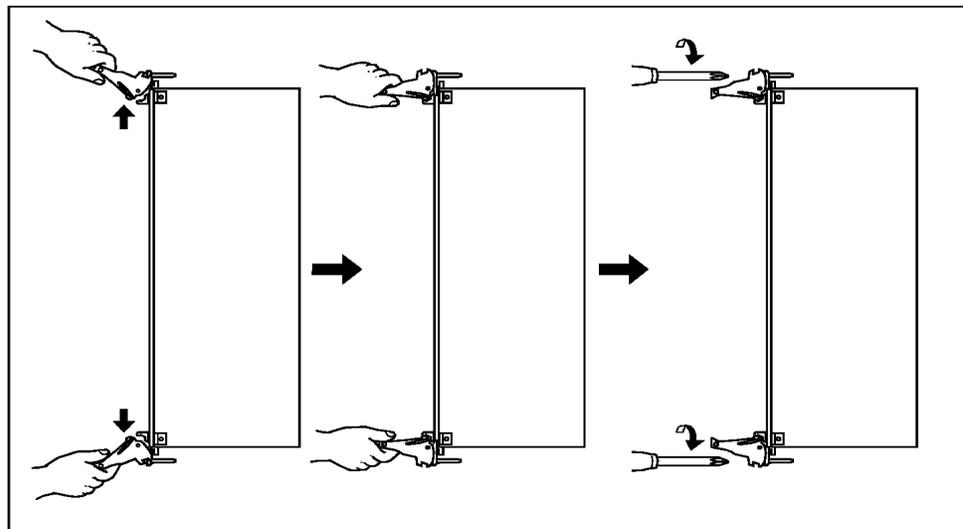
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the wrist strap grounding point, which is located on the local craft access panel (LCAP), when handling cards. This protects the cards against damage caused by static electricity.

- Label and remove all connections from the faceplate.
- 12 Loosen the attaching screws on the faulty Call Agent TM using a Phillips screwdriver.
- 13 Push the top ejector lever up and bottom ejector lever down as shown in the figure that follows, to eject the card from the shelf, and slide the card out slightly.



- 14** Insert the replacement Call Agent TM into the chassis slot, ensuring the J3, J4, and J5 connector pins are aligned with the backplane connector pins, and tighten the attaching screws using a Phillips screwdriver as shown in the figure that follows.

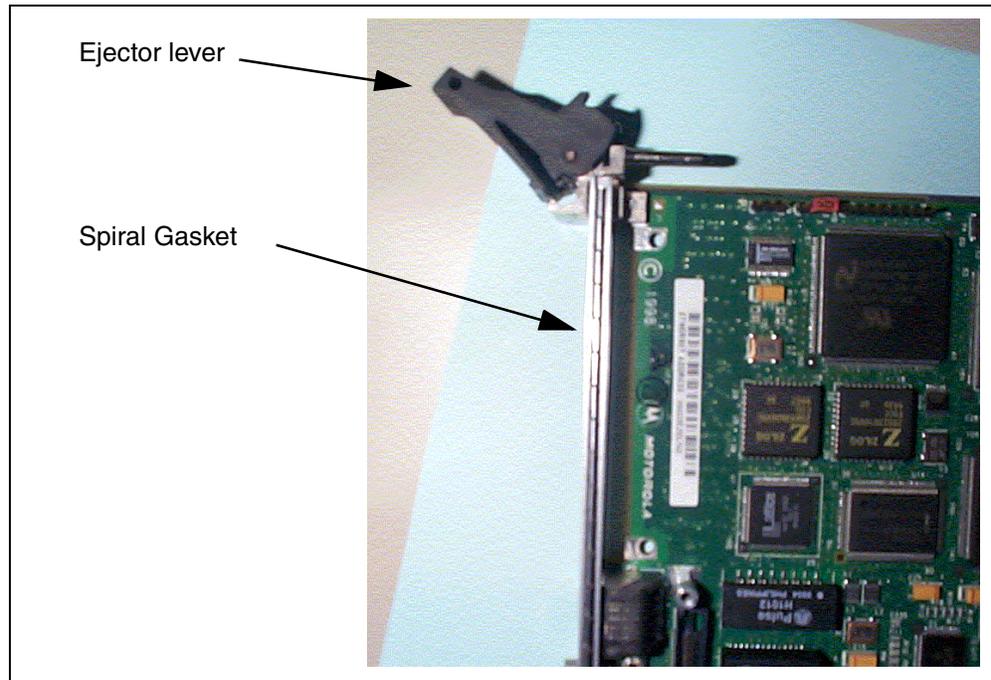
Note: Do not push on the faceplate to seat the card.



- 15** Replace all faceplate connections.

At the front of the SAM21 frame

- 16** Examine the Call Agent card before inserting it back into the SAM21 chassis to ensure that the spiral gasket is seated and not loose.



17

**CAUTION****Possible service interruption**

A service outage can occur if care is not taken while inserting the circuit pack.

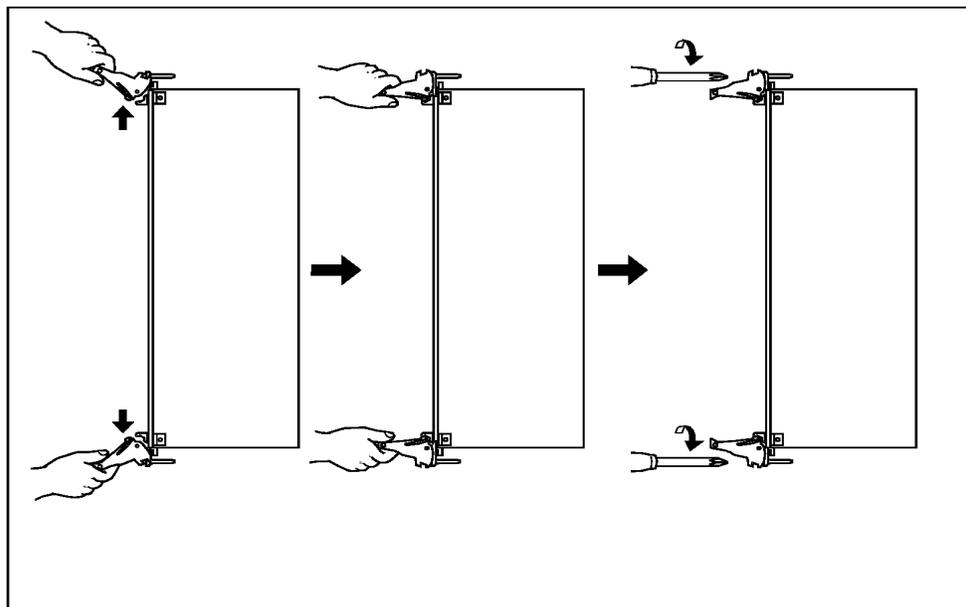
The spiral gasket, located on the faceplate of the circuit pack, can become caught on an adjacent card and ripped off of the faceplate. If the spiral gasket ends up making contact with the backplane inside the chassis, an electrical short circuit can result in a service outage.

Hold the Call Agent card by the ejector levers and insert the card back into the shelf.

Note 1: Do not push on the faceplate to seat the card.

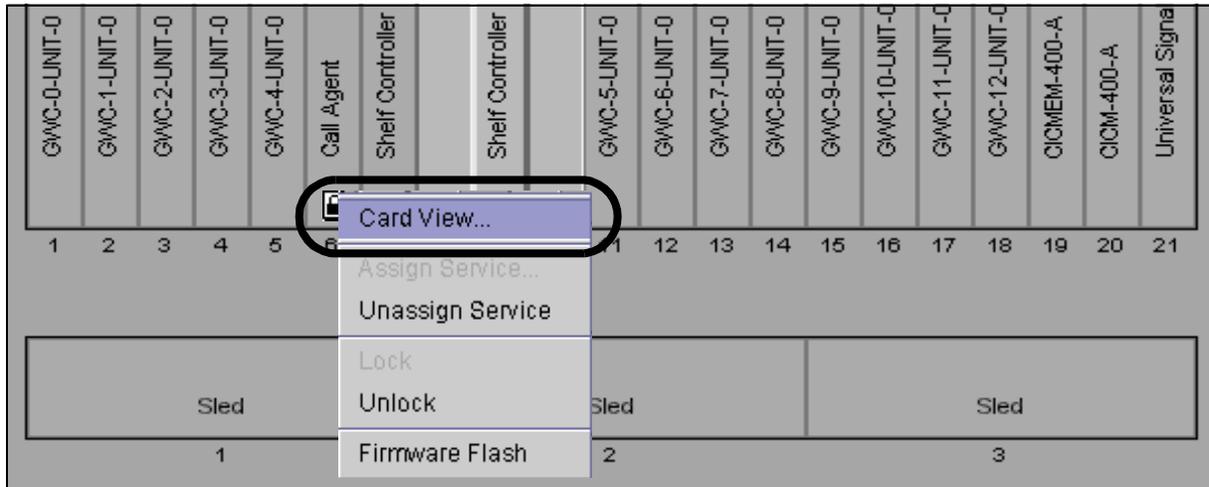
Note 2: Verify that the CPU LED lights. If the CPU LED does not light, reseal the card. If the CPU LED fails to light a second time, replace the card.

18 Secure the card by tightening the captive screws at the top and bottom of the panel as shown in the figure that follows.

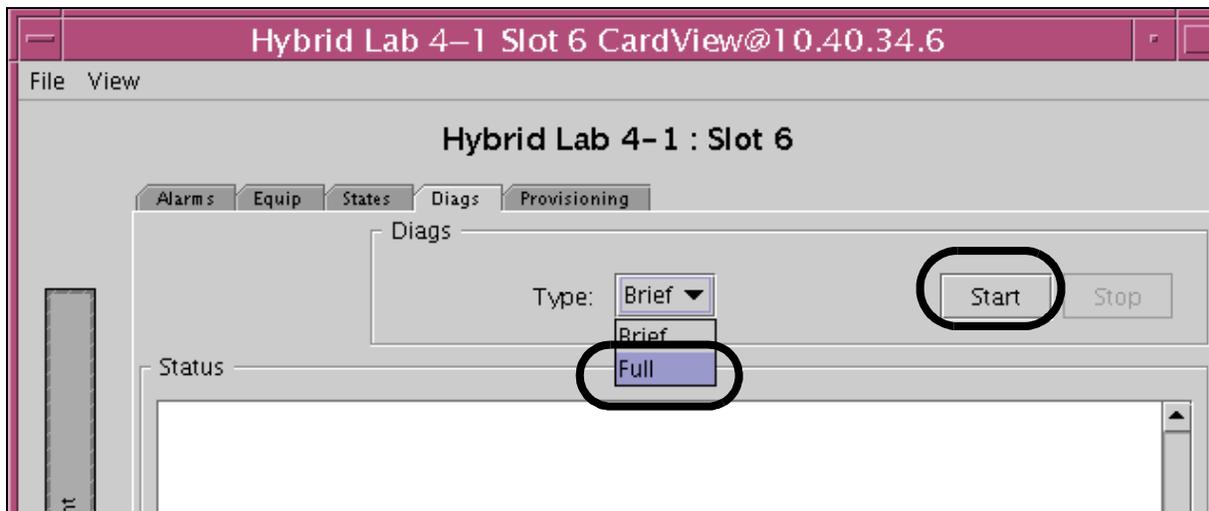


At the CS 2000 SAM21 Manager client workstation

- 19** Run full diagnostics on the replacement card. Right-click on the card icon in the Shelf View and select Card View from the context menu to open the Card View window.



- 20** Click on the Diagnostics tab from the Card View, select Full, and then click Start.

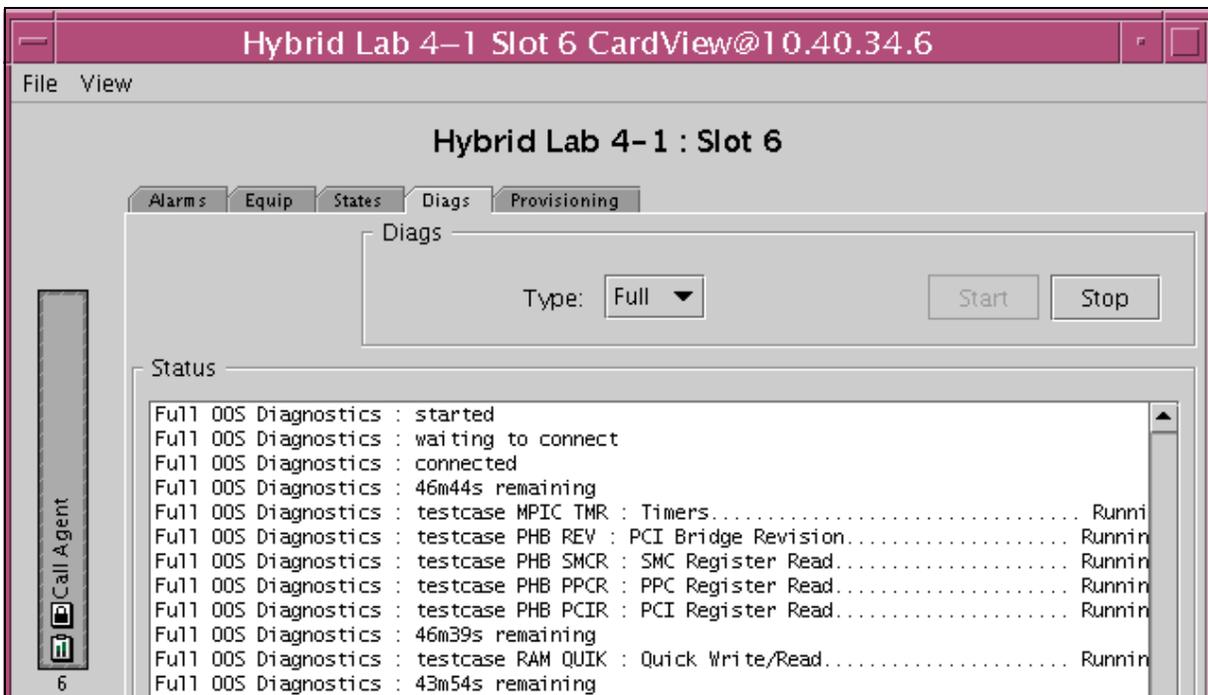


A confirmation dialog appears.

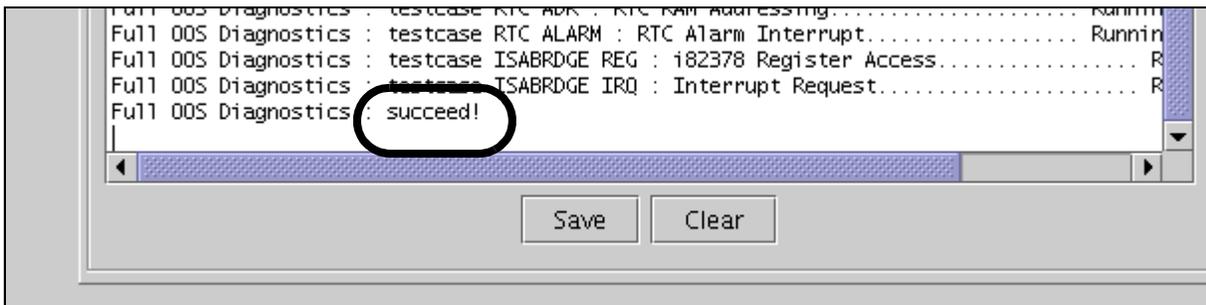


Click Yes to confirm you want to continue.

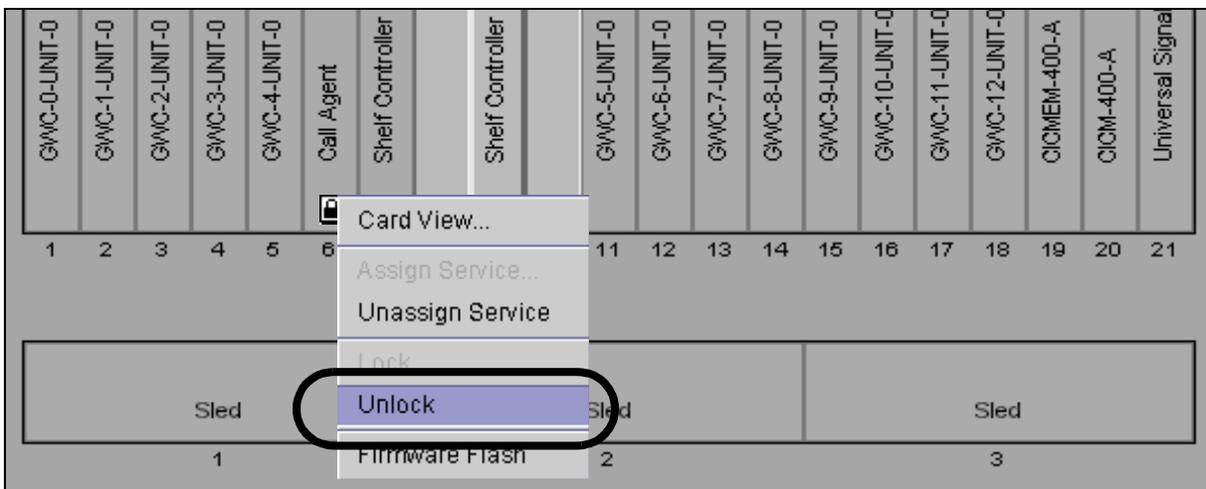
The diagnostics begin and are printed to the Status text area.



Wait for the diagnostics to complete and verify that the last line of the diagnostic output indicates "succeed!" If diagnostics do not indicate success, retry brief diagnostics and then full diagnostics. If diagnostics fail a second time, replace the card.



- 21 Right click on the card icon and select Unlock from the Shelf View. Optionally monitor the download from the States tab of the Card View window.



Note: If the Firmware Flash enable checkbox is checked on the Provisioning tab of the Card View, the Firmware Flash option is not available from the card context menu.

- 22 Wait for the lock icon to disappear from the Call Agent card on the Shelf View.

At the Call Agent Manager

- 23 Synchronize the call processing application images from the Appl level.

Telnet to the active core and enter your user ID and password.

```
ccamt
CoreMtc
Appl
Sync
```

Note: The simplex alarm clears from the alarm banner and the application flags indicate `insync`.

| | | | | | | |
|-----------|-------|-------|--------|---------|---------|------------|
| CallAgent | SYS | CON | APPL | Unit: 0 | | |
| JInact | . | . | . | | | |
| Appl | | Jam: | Link0: | Link1: | BLnk: | FC: Appl |
| 0 Quit | Unit0 | Act | no | . Act | . Inact | . insync . |
| 2 ImgTst | Unit1 | Inact | yes | . Act | . Inact | . insync . |

- 24** Release the jam on the inactive unit from the CAMtc level.

CoreMtc

CAMtc

RelJam

Note: The JInact alarm clears from the alarm banner.

- 25** Check the JF and Dlog status, and restart the subsystems if necessary.
- 26** This procedure is complete.

Perform a maintenance switch of activity on a Call Agent

Use this procedure to execute a switch of activity on a Call Agent.

At the active Call Agent Manager

- 1 Access the CoreMtc level by typing
 > **CoreMtc**
- 2 Access the Appl level by typing
 > **Appl**
- 3 Drop call processing application synchronization by typing
 > **DpSync**

```

CallAgent      SYS      CON      APPL      Unit: 0
  JInact        .        .        simplx
                M
Appl
0 Quit         Unit0  Act     no      . Inact . Act   .  NA  nosync .
2 ImgTst      Unit1  Inact   yes     . Act  . Inact .  NA  nosync /restart
3 Sync
4 DpSync
5
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP    DpSync:  Drop application synchronization.
16                               Parns: [RestartType]
17 Help                               Restart - ( WARM | COLD | RELOAD | NORESTART )
18 Refresh                               (default) - COLD
    mtc
Time 12:25

```

At the MAP

4 Execute LIMITED_PRESWACT:

```
> BCSUPDATE; LIMITED_PRESWACT
```

The LIMITED_PRESWACT command presents a warning:

```
Limited_Preswact should not be used for  
BCSUPGRADE SWACTs. Do you wish to continue?  
Please confirm ("YES", "Y", "NO", or "N"):
```

5 Confirm the warning with a Y.

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated as follows:

```
Total execution time for all complete procedures  
00:07:31.362  
All LIMITED_PRESWACT steps completed  
successfully.
```

6

**CAUTION****Possible loss of service**

NORESTARTSWACT does not check if the inactive Call Agent is unjammed. If the inactive Call Agent is jammed and a NORESTARTSWACT is requested, service is affected. Verify that the inactive Call Agent is not jammed.

**CAUTION****Possible loss of service**

Use the Call Agent Manager to verify that the inactive Call Agent does not have any critical alarms. A critical alarm causes the NORESTARTSWACT to fail. Check the GUIs for CCA, SAM21 EM and Ethernet Routing Switch 8600, and clear any alarms for those devices before proceeding with NORESTARTSWACT.

Check status:

> **BCSUPDATE; SWACTCI; STATUSCHECK**

Success is indicated as follows:

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

7 Execute the NORESTARTSWACT:

> **NORESTARTSWACT**

Note 1: Only simple two-port and echo calls that are in a stable talking state (that is, not in a transition state such as dialing) survive a CC WarmSWACT. Survival means that the call is kept up until the next signaling message is received (usually, for example, a terminate message, but on any other message as well, such as an attempt to use the conference feature).

Note 2: Attendant Consoles will be in night service after the SWACT if the INSV field is set to Y in table ATTCONS (Attendant Consoles).

Progress is printed and the process stops to verify that the inactive Call Agent is not jammed:

```
Beginning SWACT checks:
All the SWACT checks have finished successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default setting>.
Device matching during CC WARM SWACT Enabled.
Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
>
```

- 8** Confirm the warning with a **Y** if the only alarm is an APPL simplx.
The final progress follows. Activity also switches at the Call Agent Manager.

Please confirm ("YES", "Y", "NO", or "N"):

>**Y**

All Pre-SWACT checks completed. Starting Warm SWACT now.

```
***** The cursor will not be returned *****
***** unless a critical failure occurs. *****
***** Now monitoring Warm SWACT messages.*****
```

```
Pre-initialization done
Communication established
Exchange of data with the mate done
Transfer of data done (FASPECT)
Data estimation done
```

- 9** The telnet session to the active call processing application is lost. Reestablish the connection.

- 10** Execute POSTSWACT:

> **BCSUPDATE;POSTSWACT**

POSTSWACT begins, steps execute, and complete.

POSTSWACT stops at step BEGIN_TESTING:

```
REACTIVATE_TRIGASGN           executing
REACTIVATE_TRIGASGN           complete

DIRP_RECOVERY                 executing
DIRP_RECOVERY                 complete
...
BEGIN_TESTING                 executing
BEGIN_TESTING                 complete
Enter Postswact after office testing has been
completed
```

- 11** Enter the POSTSWACT command again:

> **BCSUPDATE;POSTSWACT**

```
CCA_SYNC executing
Do you want to sync the Call Agent at this time?
Please confirm ("YES", "Y", "NO", or "N"):
```

- 12** Confirm you want to sync the Call Agent with a **Y**.
A series of steps execute and complete following the SYNCing of the Call Agents.
- The final warning is printed:*
- Do you wish to erase all SFDEV file(s) ending in '\$PATCH' ?
Please confirm ("YES", "Y", "NO", "N"):
- 13** Reject deleting patch files from sfdev with a **N**.
You have completed this procedure.

Returning a Call Agent card to Nortel

Application

Use this procedure to return a card to Nortel for repair or replacement in North America.

Different telephone operating companies may have different service level agreements with Nortel. Contact your Nortel account representative to determine your service level.

Nortel Global Repair Services is available in North America:

- **phone**

Call 1-800-4NORTEL (1-800-466-7835). Listen carefully to the menu prompts. Input 1 for ERC (Express Routing Code), and then input the ERC for the repair destination. The ERC for the United States of America is 181. The ERC for Canada is 1142.

- **FAX**

In the United States of America, 972-685-8862. In Canada, 1-877-618-2204.

All FAX orders are returned with an RMA # by the next business day. Faxed emergency orders must also be called in to ensure the receipt of FAX.

- **electronic mail**

In the United States of America, rich.repair@nortel.com. In Canada, canentry@nortel.com.

To obtain an E-mail Parts Request Form, send an E-mail to one of the above addresses and include "PRF" in the subject/title field and a form will be sent automatically. Record the customer PO in the subject/title field when E-mailing the completed Parts Request Form. All E-mail orders are returned with an RMA # by the next business day.

Interval

Perform this procedure as required.

Common procedures

There are no common procedures.

Action

Contact Nortel by one of the methods above, and follow the instructions provided.

Replacing a BIP alarm module

Application

Use this procedure to replace a breaker interface panel (BIP) alarm module.

The following frames contain an alarm module:

- Services Application module Frame (SAMF) for CS 2000 and CS 2000 Compact
- Cabinetized Operations Administration and Maintenance (COAM) frame for CS 2000 and CS 2000 Compact
- Call Control Frame (CCF) for CS 2000 Compact only
- Ethernet Routing Switch (ERS) 8600 Carrier Voice over IP Frame, which is also referred to as the CS LAN Frame, for CS 2000 and CS 2000 Compact
- Universal Signaling Point (USP), which can be one of USP Compact CCF, USP Frame with a Control Application Module (CAM) shelf, or USP in a COAM

Interval

Replace a BIP alarm module when the module fails.

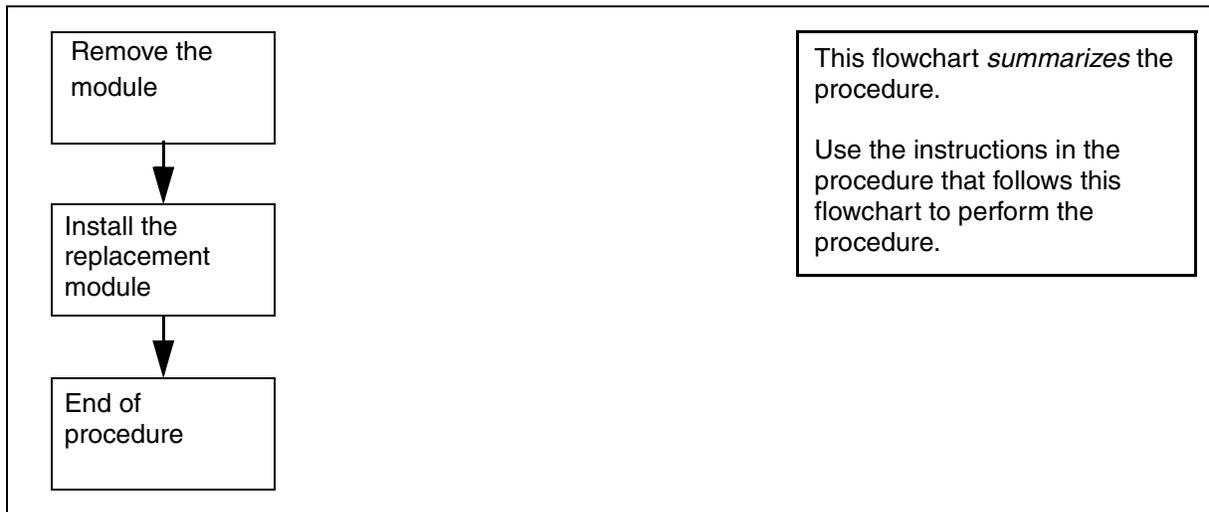
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Replacing a BIP alarm module



WARNING

Risk of static electricity damage

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).



CAUTION

Loss of service

Read and make sure you thoroughly understand the instructions in this procedure before replacing the BIP alarm module. While the module is removed, alarm reporting is temporarily suspended.

At the front of the BIP

- 1** Remove the failed BIP alarm module. To remove the module, use the procedure [Removing a BIP alarm module](#). When the module has been removed, proceed to [step 2](#) of this procedure.
- 2** Install the replacement BIP alarm module. To replace the module, use the procedure [Installing a BIP alarm module](#).
- 3** This procedure is complete.

Removing a BIP alarm module

Application

Remove a BIP alarm module to replace it due to a failure or to ensure safe removal of the BIP.

Interval

Remove a BIP alarm module when the module fails.

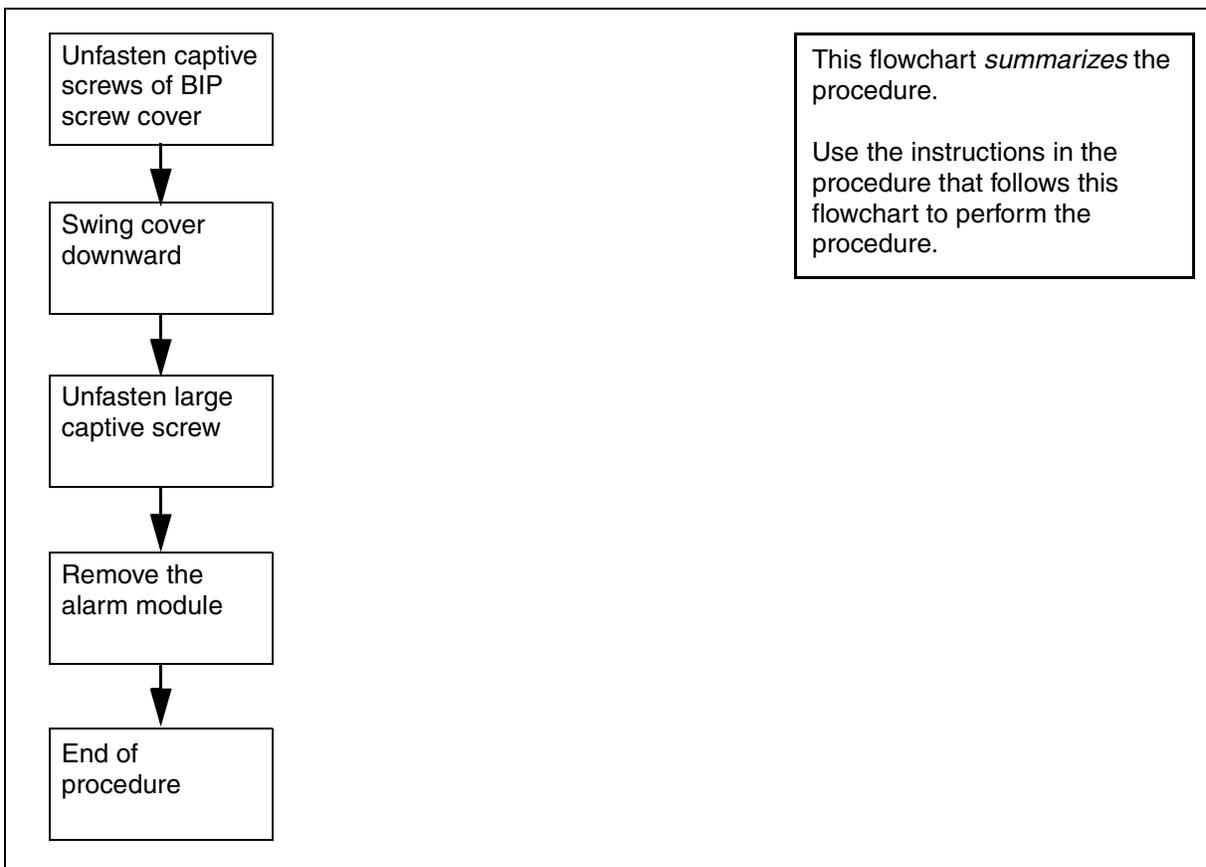
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Removing a BIP alarm module



**WARNING****Risk of static electricity damage**

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).

**CAUTION****Loss of service**

Read and make sure you thoroughly understand the instructions in this procedure before removing the BIP alarm module. While the module is removed, alarm reporting is temporarily suspended.

At the front right side of the BIP

- 1 Unfasten the slotted captive screws of the BIP screw cover.
- 2 Swing the cover downward.
- 3 Unfasten the large captive screw of the BIP alarm module.
- 4 While pinching the lower front lip of the module with your thumb and finger tips, pull gently but firmly straight out until the alarm disengages. Stop pulling when the front of the module is past the front of the BIP.
- 5 Pull the module straight out of the BIP.
- 6 This procedure is complete.

Installing a BIP alarm module

Application

The BIP alarm module indicates hardware alarms, drives the alarm light-emitting diode (LED) board and monitors the state of the power breakers.

Interval

Install a BIP alarm module as part of a replacement or initial installation task.

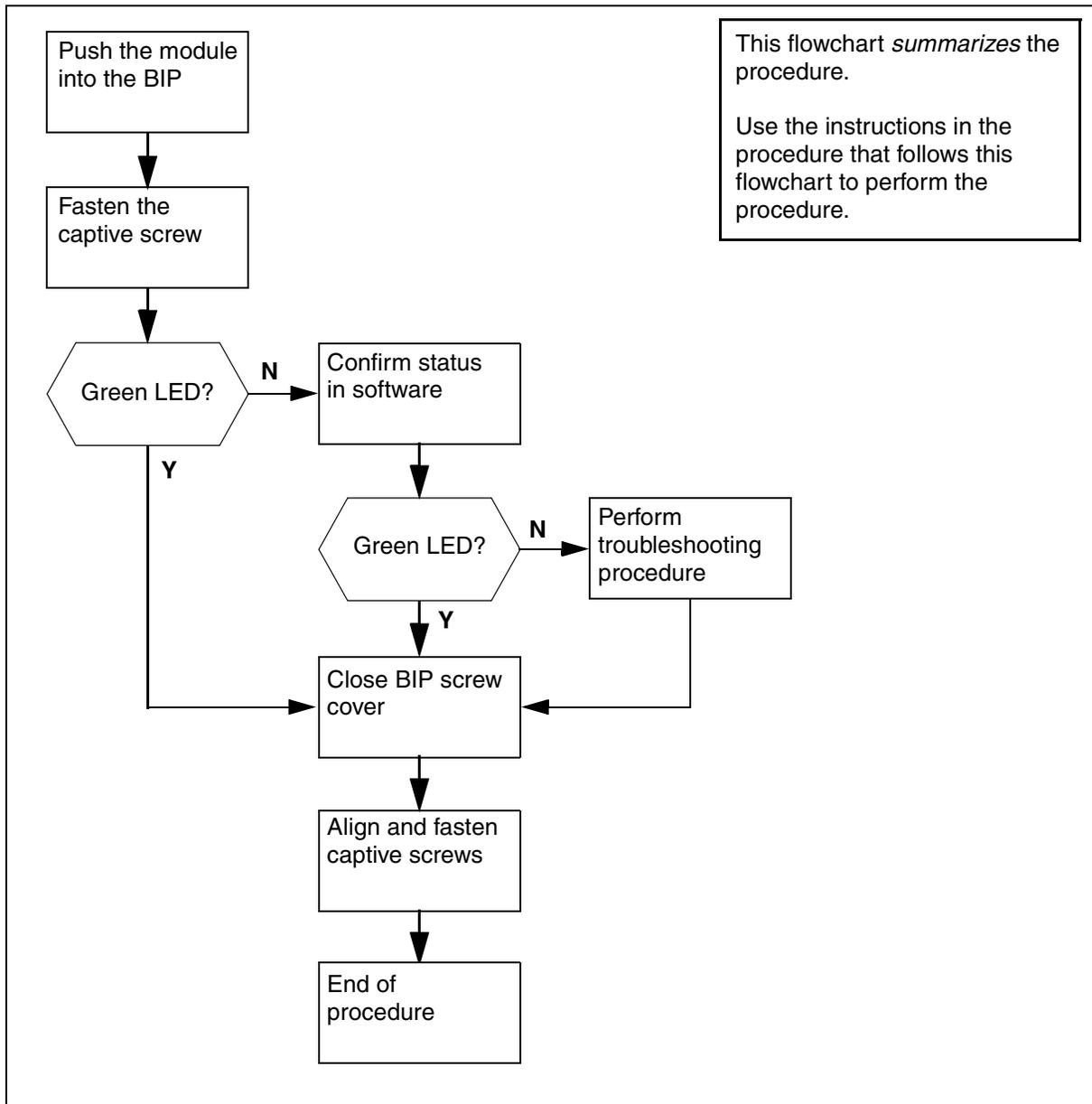
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Installing a BIP alarm module



WARNING

Risk of static electricity damage

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).



CAUTION
Loss of service

Read and make sure you thoroughly understand the instructions in this procedure before removing the BIP alarm module. To minimize the effect of removing an alarm module, insert the replacement immediately. Once the alarm module is installed, software alarms stop.

At the front of the BIP

- 1 Get a BIP alarm module PEC NTRX51HC.
- 2 Grip the replacement alarm module with the fingers and thumb of one hand on the lower front lip (the screw end) and use the other hand to align the rear of the module with the opening in the BIP.
- 3 Push the module gently but firmly straight in until it engages. Stop pushing when the front of the module is flush with the front of the BIP.
- 4 Engage and fasten the large slotted captive screw of the alarm module. Do not strip the threads or the hole because the module cannot seat properly.
- 5 Check the alarm module status LEDs.

| If the color is | Do |
|------------------|------------------------|
| green | step 7 |
| other than green | step 6 |

- 6 Have the network operator confirm the status in the software.

| If the color is | Do |
|------------------|---|
| green | step 7 |
| other than green | Perform troubleshooting procedures to clear the problem, and continue to step 7 . |

- 7 Close the BIP screw cover upwards.
- 8 Align and fasten the slotted captive screws of the cover.
- 9 This procedure is complete.

Replacing cooling unit fan filters

Application

Use this procedure to replace cooling unit fan filters for the SAM21 shelf. The part number of the cooling unit fan filter is A0828397.

The cooling unit fan filter is foam. Access the cooling unit fan filter from the front of the SAM21 shelf. Cooling units are in the lower front section of the SAM21 shelf.

Interval

Replace the cooling unit fan filters every 10 000 hours.

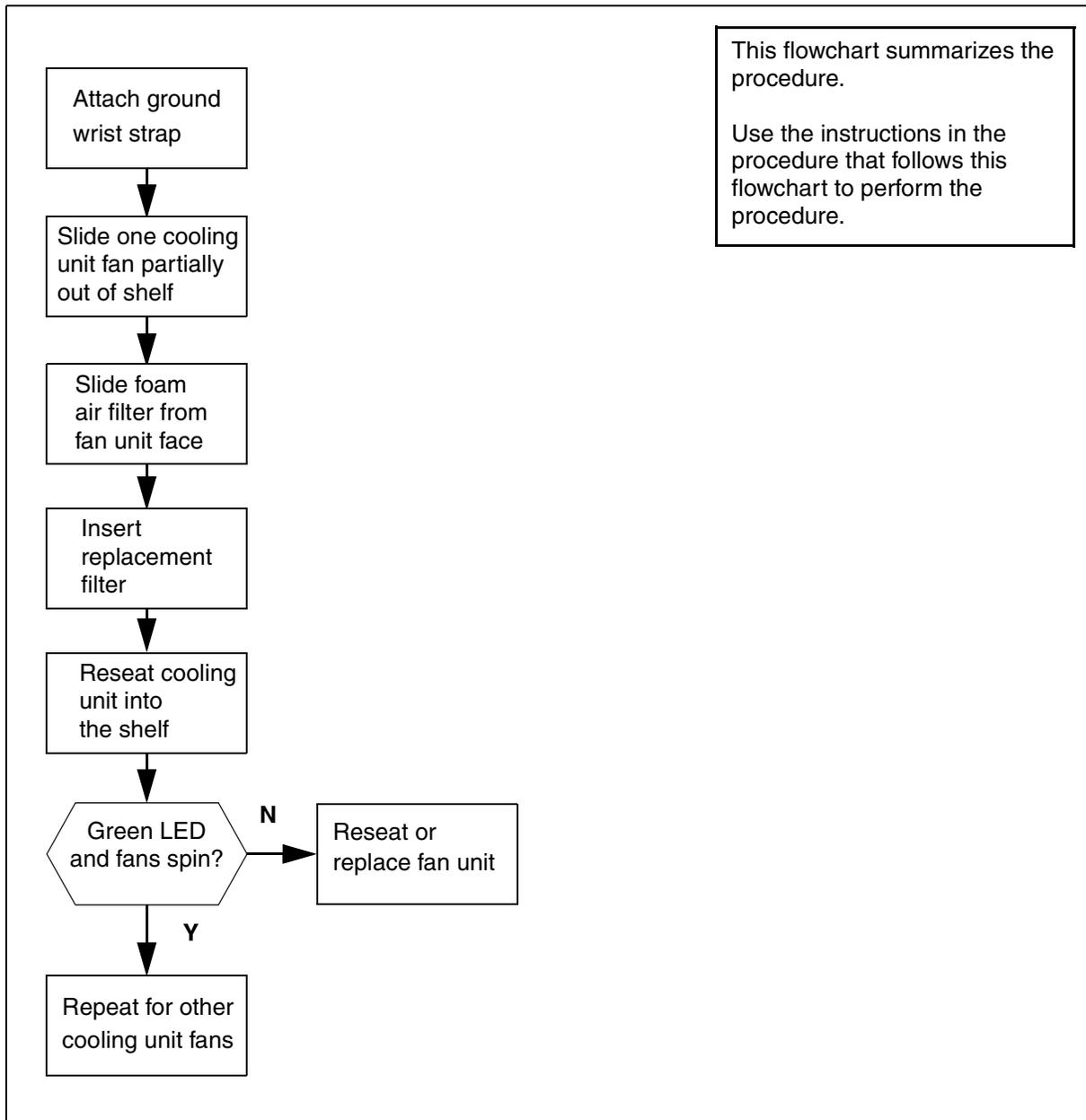
Common procedures

There are no common procedures.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Replacing cooling unit fan filters



**WARNING****Risk of static electricity damage**

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).

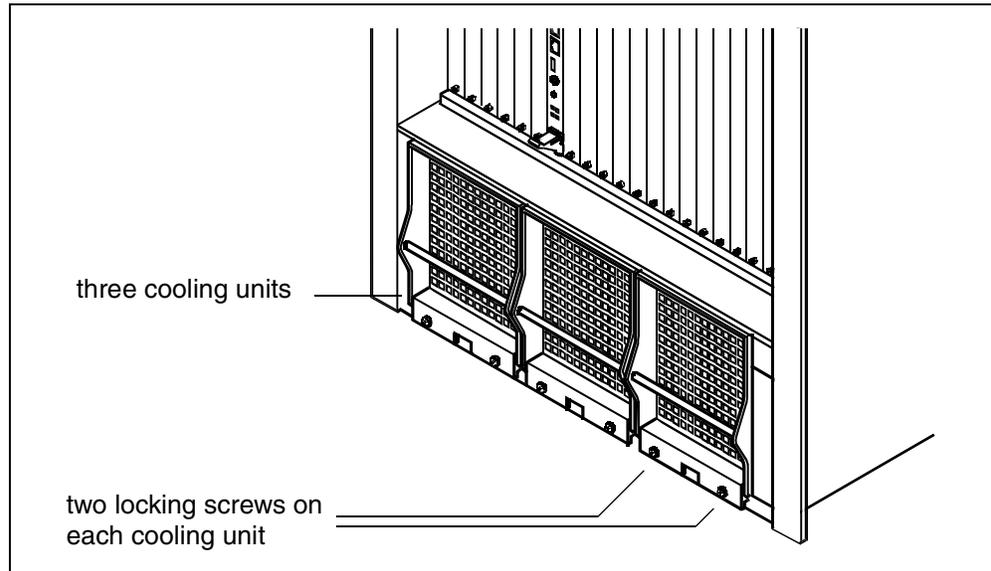
**CAUTION****Loss of service**

Read and make sure you thoroughly understand the instructions in this procedure before performing the filter replacement. Do not allow the cooling unit to remain without power for more than one minute. Do not unseat more than one cooling unit at a time.

At the SAM21 shelf

- 1 Get a new, replacement cooling unit fan filter (part number A0828397). Do not re-use old filters.
- 2 Open any doors on the cabinet completely.
- 3 Locate the following in the lower front section of the cabinet.
 - Three cooling units for each SAM21 shelf.
 - One foam cooling unit fan filter on the face of each cooling unit.

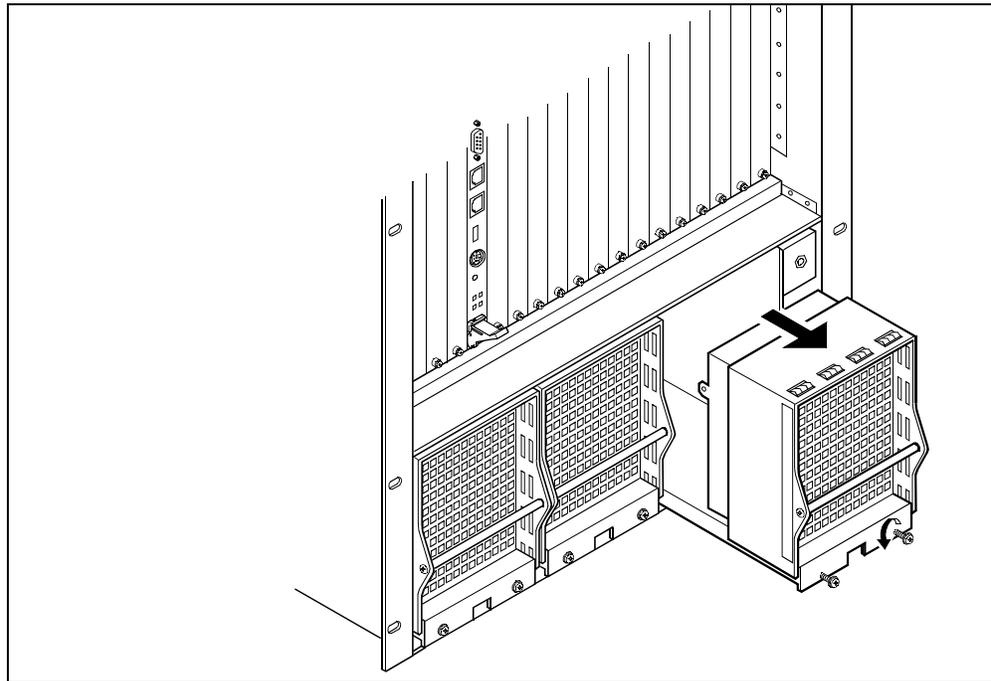
SAM21 shelf cooling unit fan locations



- 4 Pull one of the three cooling units partially away from the shelf. Wait 30 seconds to allow the fan to spin down.

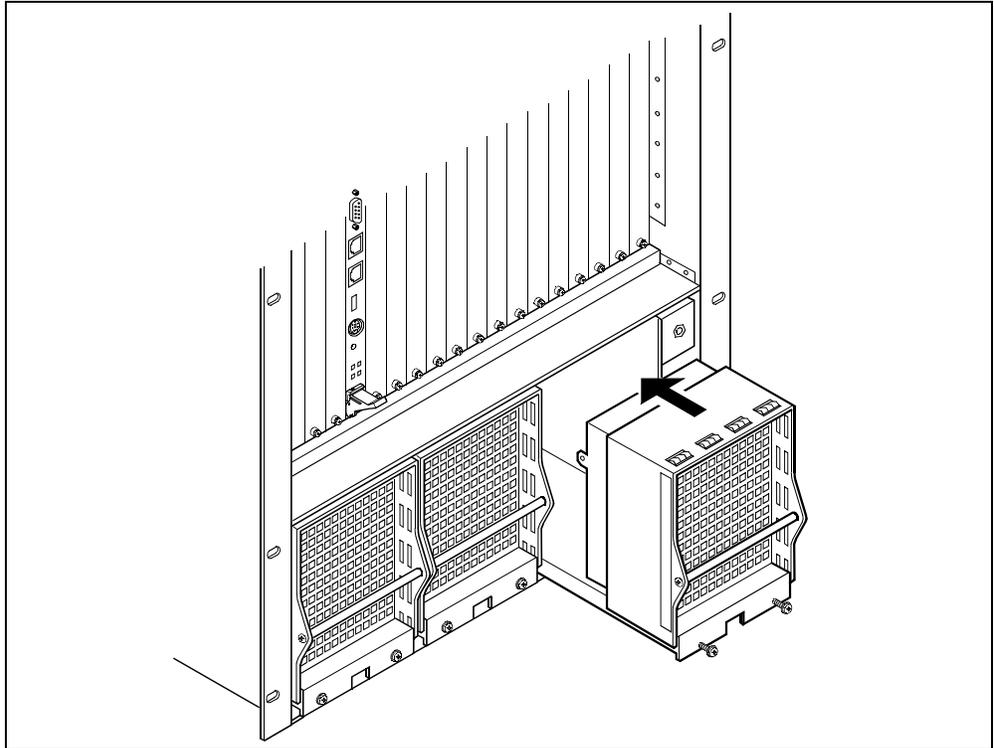
Note: The FSP blower LED will light. A major alarm appears on CS 2000 SAM21 Manager client. Two of the cooling units also supply power to the shelf. An additional major alarm is raised when either of these cooling units is removed.

Unseat one cooling unit



- 5 Remove the foam air filter by pinching the filter in the center so that the edges of the filter slip out of the filter retainer. Lift the foam air filter out and over the cooling unit handle.
- 6 Insert the replacement cooling unit filter. Tuck the edges of the foam air filter behind the filter retainer.
- 7 Reseat the cooling unit.

Reseat the cooling unit



- 8 Make sure that the fan powers up. Make sure that the green LED lights on the cooling unit.
If the green LED does not light or the fan does not spin, reseal the cooling unit. If the green LED does not light or the fan does not spin a second time, replace the cooling unit. If the green LED does not light or fan does not spin on the replacement unit, contact Nortel support personnel.
- 9 Tighten the locking screws on the cooling unit. Turn the locking screws in a clockwise direction.
- 10 Repeat for each cooling unit. Disconnect the wrist strap lead from the FSP when all air filters are replaced.
- 11 This procedure is complete.

Testing wrist-strap grounding cords

Application

Use this procedure to test the resistance of wrist-strap grounding cords. The resistance must have minimum and maximum values as follows:

- resistance must be low enough to allow static electricity to discharge from the human body
- resistance must be high enough to prevent electrocution if the equipment develops a short circuit

Interval

Perform this procedure every 30 days (monthly).

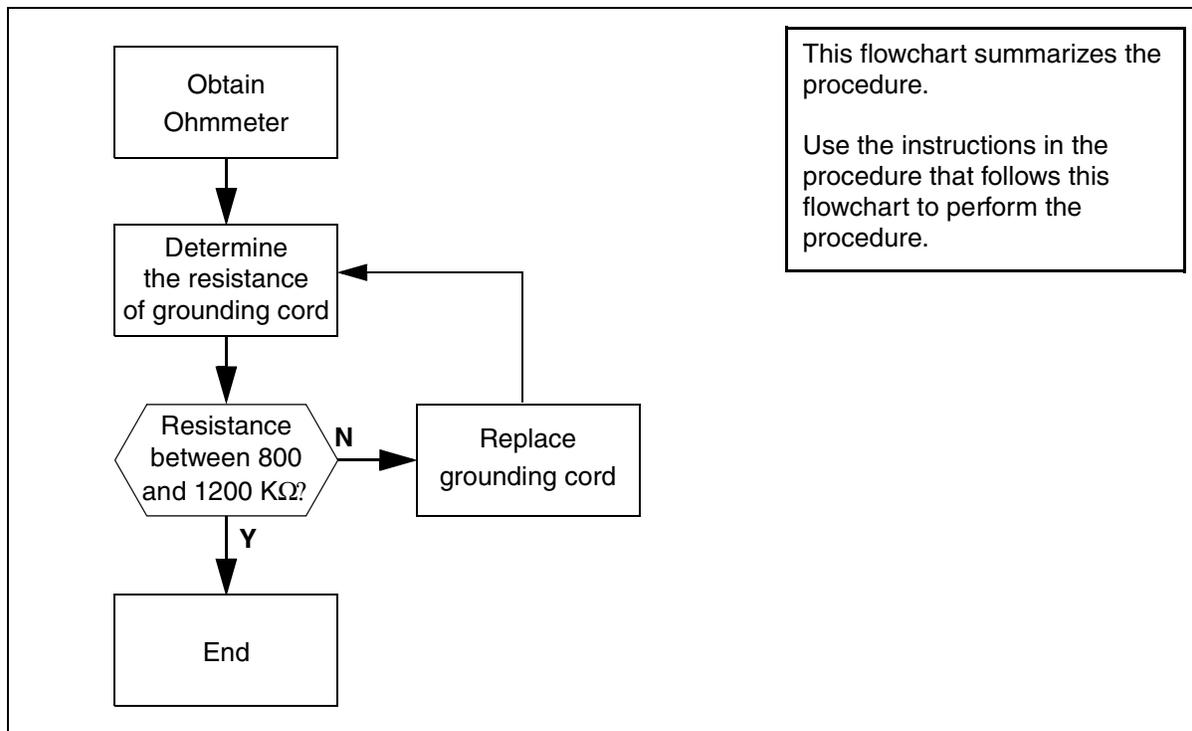
Common procedures

There are no common procedures.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Testing wrist-strap grounding cords



**DANGER****Risk of electrocution**

Do not use a grounding cord with a resistance less than 800K ohm. A resistance lower than 800K ohm opens you to the risk of electrocution. Electrocution can occur if the equipment short-circuits while you are wearing the wrist strap.

**WARNING****Risk of static damage to electronic equipment**

Do not use a grounding cord with a resistance greater than 1200K ohm. A resistance greater than 1200K ohm cannot conduct static charges correctly to ground nor protect electronic equipment against possible damage from electrostatic discharge.

At the equipment frame

- 1 Get an ohmmeter.
- 2 Disconnect the grounding cord from the wrist strap.
- 3 Use the ohmmeter to measure the resistance between the opposite ends of the grounding cord.

If the resistance is**Do**

between 800K ohm and 1200K ohm [step 7](#)

less than 800K ohm or greater than 1200K ohm [step 4](#)

- 4 Discard the grounding cord that has faults.
- 5 Get a new grounding cord.
- 6 Test the new grounding cord.

If the resistance is**Do**

between 800K ohm and 1200K ohm [step 7](#)

less than 800K ohm or greater than 1200K ohm [step 4](#)

- 7 Connect the wrist strap to the grounding cord again.
- 8 You have completed this procedure.

Call Agent Manager alarm clearing procedures

Use this procedure to begin diagnosis of the Call Agent from the Call Agent Manager.

To use the Call Agent Manager, ensure that the PassThru feature is provisioned on the CS 2000 Core Manager.

At the Call Agent Manager

- 1 Enter the CoreMtc level.

CoreMtc

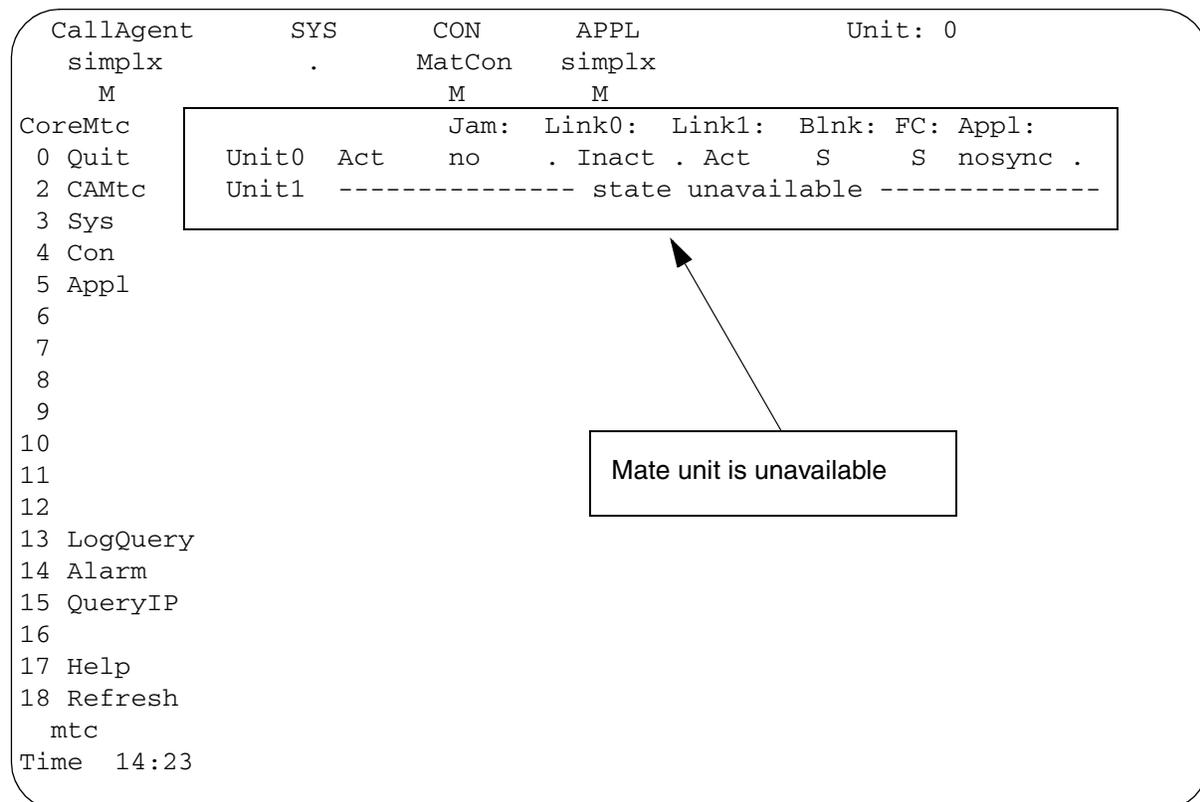
- 2 Review the following figures to determine if the mate unit is available.

Call Agent Manager screen when mate unit is unavailable

```

CallAgent      SYS      CON      APPL      Unit: 0
  simplx      .      MatCon  simplx
    M
CoreMtc
0 Quit      Unit0 Act   no      . Inact . Act   S      S nosync .
2 CAMtc     Unit1 ----- state unavailable -----
3 Sys
4 Con
5 Appl
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh
   mtc
Time 14:23

```



The screenshot shows the Call Agent Manager interface. The top line displays 'CallAgent Unit: 0'. Below it, the status of various components is shown: 'simplx . MatCon simplx' and 'M M M'. The 'CoreMtc' section shows a list of options: '0 Quit', '2 CAMtc', '3 Sys', '4 Con', '5 Appl', '6', '7', '8', '9', '10', '11', '12', '13 LogQuery', '14 Alarm', '15 QueryIP', '16', '17 Help', '18 Refresh', and 'mtc'. The 'Time' is '14:23'. A box highlights the error message: 'Unit1 ----- state unavailable -----'. An arrow points from a box labeled 'Mate unit is unavailable' to this error message.

Call Agent Manager screen when mate is available and alarms are active

```

CallAgent      SYS      CON      APPL      Unit: 0
.              NTP      .        .
CoreMtc
0 Quit
2 CAMtc       Unit0 Act   no      . Inact . Act   .      . insync .
3 Sys
4 Con
5 Appl
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh
   mtc
Time 14:23
    
```

A dot indicates that services are operating normally.

If an alarm appears, the dot is replaced with an abbreviation for the alarmed subsystem. Below the abbreviation, "M" indicates a major alarm and "*C*" indicates a critical alarm. Otherwise, the alarm is of minor severity.

| If | Do |
|--------------------------------|---|
| the mate unit is unavailable | Proceed to CS 2000 SAM21 Manager procedures on page 169 |
| alarms are in the alarm banner | go to step 3 |

- 3** Clear Call Agent alarms.
- 4** Clear SYS alarms.
- 5** Clear CON alarms.
- 6** Clear APPL alarms.
- 7** This procedure is complete.

Additional information

The alarm banner shows the most severe faults and can mask lesser faults. To determine all faults in a level enter the alarm command with the level:

Alarm con

Call Agent Manager screen with masked alarms

```
CallAgent      SYS      CON      APPL      Unit: 0
.              .        MatCon    simplx
                M        M

CCAMtc
0 Quit
2 CoreMtc
3 Admin
4
5
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
   mtc
Time 10:34 >
```

```
CON alarms for unit 0:

  Alarm Severity Description
LnkCon major Link0: INSV, mateCon: UNAVAIL, netCon: AVAIL;
Link1: INSV, mateCon: UNAVAIL, netCon: AVAIL;
BLink: SYSB, mateCon: UNAVAIL;
FC: SYSB;

MatCon major Link0: INSV, mateCon: UNAVAIL, netCon: AVAIL;
Link1: INSV, mateCon: UNAVAIL, netCon: AVAIL;
BLink: SYSB, mateCon: UNAVAIL;
FC: SYSB;

CON alarms for unit 1: none
```

In the figure above, a mate connectivity alarm masked a linked connectivity alarm. However, the alarm banner indicates the most severe alarm. Clear the most severe alarm first.

Retrieving logs

Use this procedure to retrieve platform log reports.

At the Call Agent Manager

- 1 Enter the LogQuery command.

LogQuery [numLogs | ALL] [MATE]

[numLogs|ALL]

Use this optional parameter to specify the number of log reports to display, 1 to 50. The ALL parameter displays up to 50 log reports. The default behavior is to display 20 log reports.

[MATE]

Use this optional parameter to display the log reports for the mate unit.

```

CallAgent      SYS      CON      APPL      Unit: 0
.              NTP      .        simplx
               M              M
CCAMtc        CCA631 JUL25 10:46:49 INFO Mate Connectivity Restored
0 Quit        Unit Number : 0, ACTIVE
2 CoreMtc     Description : Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
3 Admin      Link1: INSV, mateCon: AVAIL, netCon: AVAIL;
4            BLink: INSV, mateCon: AVAIL; FC: INSV;
5
6            CCA651 JUL25 10:46:49 INFO Mate Communication Restored
7            Unit Number : 0, ACTIVE
8            Description : Mate unit is available.
9
10           * CCA331 JUL25 10:46:48 FLT Mate Connectivity
11           Unit Number : 0, ACTIVE
12           Description : Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
13 LogQuery   Link1: INSV, mateCon: AVAIL, netCon: AVAIL;
14 Alarm      BLink: SYSB, mateCon: UNAVAIL; FC: INSV;
15
16           CCA635 JUL25 10:46:47 INFO Link Connectivity Restored
17 Help       Unit Number : 0, ACTIVE
18 Refresh    Description : Link0: INSV, mateCon: UNAVAIL, netCon: AVAIL;
   mtc        Link1: INSV, mateCon: UNAVAIL, netCon: AVAIL;
Time 10:46   MORE... (19%)

```

- 2 This procedure is complete.

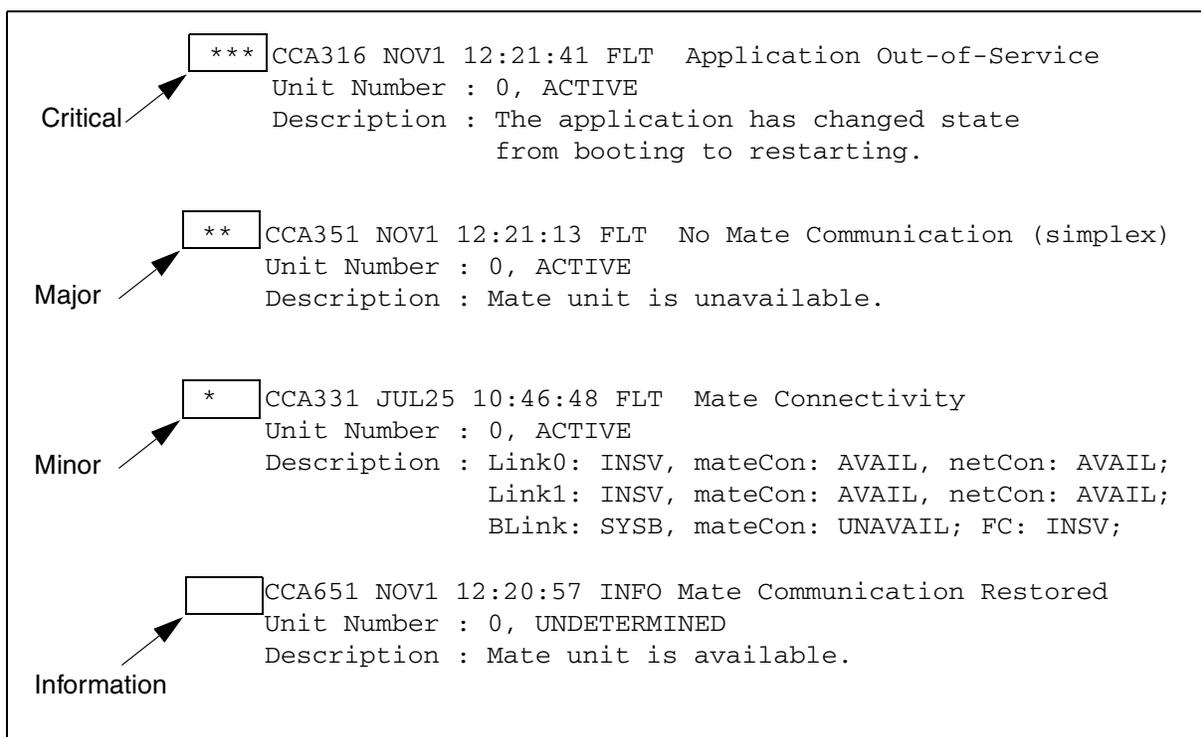
Additional information

Logs are available from the platform, the call processing application, and the Operations Support System (OSS) network.

Platform access

The procedure above shows how to retrieve platform logs from the Call Agent Manager.

Logs are categorized into four categories: critical, major, minor, and information. Refer to the following figure for examples.



Logs are also categorized by number. Refer to the figure above and the following table for more information.

| Event number | Range | Description |
|--------------|------------|---|
| Trouble | 300 to 399 | These logs indicate abnormal operation. They can be alarms or alerts. |
| Information | 600 to 699 | These logs provide information about system events. |

Call processing application access

Call processing logs are available with the **LOGUTIL** tool within the call processing application. These logs and the platform logs are transferred to the OSS network.

Call Agent alarm and log matrix

The following table provides a cross reference to the alarms, logs, and fault severities for the Call Agent. Alarm severities are critical (C), major (M), and minor (m).

| Alarm name and clearing procedure | Severity | | | Related log reports |
|-----------------------------------|----------|---|---|--|
| | C | M | m | |
| CallAgent RExtTst | | | x | See CallAgent RExFlt |
| Call Agent RExSch | | | x | CCA365 System REx has not started for over 7 days CCA665 RExSch alarm has cleared |
| Call Agent Config | | | x | CCA375 One unit has a different CPU type than the other unit CCA675 config alarm has cleared |
| CallAgent simplx | | x | | CCA351 Node simplex CCA651 Node duplex |
| CallAgent JInact | | | x | CCA355 Inactive unit jammed CCA655 Jam released on inactive unit |
| CallAgent RExFlt | | | x | CCA362 Rex test failed CCA660 Rex test started CCA661 Rex test finished CCA663 Rex test rejected |
| CallAgent C_MisM | | | x | CCA380 Committed loads mismatch CCA680 Committed loads equal <i>Note:</i> These log reports were listed as 3PC372 and 3PC672 for SN04. |
| SYS HW Flt | x | x | | CCA309 Board fault CCA609 Board fault cleared |
| SYS NFS | x | x | x | CCA304 NFS mounts not accessible CCA604 All NFS mounts accessible |

| Alarm name and clearing procedure | Severity | | | Related log reports |
|-----------------------------------|----------|---|---|---|
| | C | M | m | |
| SYS Memory | x | x | x | CCA300 Memory usage threshold exceeded CCA600 Memory usage threshold not exceeded |
| SYS NTP | | x | x | CCA305 Unable to sync to properly to NTP server or drift is excessive CCA605 Synced properly to NTP server |
| SYS CPU Ld | x | x | x | CCA301 CPU load average threshold exceeded CCA601 CPU load average threshold not exceeded |
| SYS Disk | x | x | x | CCA302 Disk usage threshold exceeded CCA602 Disk usage threshold not exceeded |
| SYS Zombie | x | x | x | CCA303 Zombie process threshold exceeded CCA603 Zombie process threshold not exceeded |
| SYS CpuUtl | x | x | x | CCA306 CPU utilization threshold exceeded CCA606 CPU utilization threshold not exceeded |
| CON MatCon | x | x | | CCA331 Unable to talk to mate via Ethernet/fiber CCA631 Able to talk to mate via Ethernet/fiber |
| CON LnkCon | x | x | | CCA335 Ethernet interface down CCA635 Ethernet interface okay |
| CON NetCon | | x | x | CCA336 Unable to talk to network CCA636 Able to talk to network |
| APPL NoAppl | x | | x | CCA316 Application OOS CCA616 Application INSV |
| APPL ImgTst | | | x | See APPL Image |

| Alarm name and clearing procedure | Severity | | | Related log reports |
|-----------------------------------|----------|---|---|--|
| | C | M | m | |
| APPL Image | | x | | CCA322 Image test failed CCA620 Image test started CCA621 Image test finished |
| APPL simplx | | x | | CCA315 Application simplex CCA615 Application duplex |
| APPL Memory | | x | x | CCA314 Application Memory CCA615 Application Memory Alarm Cleared |

The log reports and alarms in the following table are available if the CS 2000 - Compact is configured with Message Controller cards.

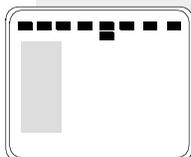
| Alarm name and clearing procedure | Severity | | | Related log reports |
|-----------------------------------|----------|---|---|---|
| | C | M | m | |
| CallAgent NIIKEY | | | x | CCA352 NIIKEY Detected CCA652 NIIKEY Removed |
| MC ATM | x | x | x | CCA340 MC ATM Connectivity CCA640 MC ATM Alarm Cleared |
| MC ETH | | x | x | CCA345 MC Ethernet Connectivity CCA645 MC Ethernet Connectivity Restored |
| MC MCTbl | | x | x | CCA344 MC Trouble CCA644 MC Trouble Alarm Cleared |

The following log reports are not correlated with alarms or alarm clearing:

- CCA390 — Process panic (Trap)
- CCA670 — SwAct failover started
- CCA671 — SwAct failover finished
- CCA685 — CCA Geo OSPF Disable
- CCA686 — CCA Geo OSPF Enable

CallAgent JInact minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
JInact        .        .        .
```

Indication

The Call Agent generates a CCA355 log report in addition to the alarm. The Call Agent generates a CCA655 log report when the alarm clears.

Meaning

The inactive unit is jammed to prevent a Switch of Activity (SWACT).

Action

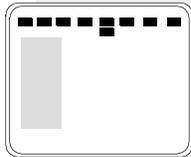
This alarm is expected during an upgrade or Call Agent card replacement. No action is required.

```
CallAgent      SYS      CON      APPL      Unit: 0
JInact        .        .        simplx

Sys
0 Quit        Unit0  Inact  yes   . Act  . Inact . . insync .
2 QryCPU     Unit1  Act    no    . Act  . Inact . . insync .
3 QryDsk
4 QryMem
5 QryZmb
6 QryNFS
7 QryLd
8 QryNTP
9 QryCpUtl
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh
   mtc
Time 14:56 >
```

CallAgent RExFit minor

Alarm display



| | | | | |
|-----------|-----|-----|------|---------|
| CallAgent | SYS | CON | APPL | Unit: 0 |
| RExFIt | . | . | . | |

Indication

The Call Agent generates a CCA362 log report in addition to the alarm. The log report indicates at what point the test failed.

Meaning

One or more tests failed. This alarm is also raised if a user manually aborts a REXtst.

The routine exercise test (REXTst) has 5 stages:

1. image test
2. sanity test
3. hardware diagnostic test
4. reset and reboot
5. call processing application synchronization

The inactive Call Agent is enabled during stages 1, 2, and 5. The inactive Call Agent is disabled for stages 3 and the beginning of stage 4. If the REXtst fails during stages 3 or 4, the inactive Call Agent is recovered by the Shelf Controller.

If the CS 2000 - Compact is configured with Message Controller cards, one Message Controller card is selected for diagnostics. The Message Controller is removed from service by a Call Agent request and then hardware diagnostics are run on the Message Controller, followed by a reset on the Message Controller. The results of the diagnostics are available in the REXtst QUERY report. If diagnostics are successful, the other Message Controller is selected for diagnostics on the next REXtst.

Action

At the Call Agent Manager

- 1 Review office records to determine if the fault has occurred in the past.
- 2 Enter the CoreMtc level.

CoreMtc

- 3 Enter the CAMtc level.

CAMtc

- 4 Query the results for the last REXtst.

RExtst QUERY

```

CallAgent      SYS      CON      APPL      Unit: 0
RExFlt        .        .        .

CAMtc
0 Quit        Unit0  Inact   no        . Act    . Inact  .      .  insync .
2 Jam        Unit1  Act     no        . Act    . Inact  .      .  insync .
3 RelJam
4 REXtst
5 SwAct
6
7
8
9
10
11           Results for QUERY LAST REX TEST:
12
13 LogQuery
14 Alarm              Initiator: MANUAL
15 QueryIP            Class: FULL
16 CA REX Last Run On: Thu Apr 10 20:07:53 2003
17 Help              CA Unit Tested: 1
18 Refresh            Result: PASSED
   mtc
Time 17:45 >

```

Note: If Call Agent cards are provisioned with Message Controller cards, the results for the last Message Controller REXtst are reported below the Call Agent information.

- 5 Run a manual RExTst during a period of low traffic to determine if the fault is intermittent.

CoreMtc
CAMtc
RExTst RUN

- 6 Determine the next action.

| If | Do |
|-----------------------------|---|
| the fault does not reappear | record the fault in office records |
| the fault does appear | Gather TRAP, SWER, footprint buffer information and contact Nortel support personnel. |

- 7 This procedure is complete.

Additional information

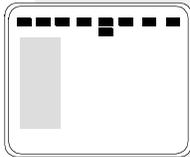
Use the following procedure to gather TRAP log reports, SWER log reports, and footprint buffer information.

At the MAP interface

- 1 Record the session.
CI:> RECORD START ONTO SD00TEMP
- 2 Enter the log utilities level and print TRAP and SWER log reports.
CI:> LOGUTIL;OPEN TRAP;BACK ALL;OPEN SWER;BACK ALL;QUIT
- 3 Enter the footprint level and print the active buffers for the active and inactive call processing applications.
CI:> FOOTPRT;FPBUF ACTIVE T;FPBUF ACTIVE M;QUIT
- 4 Stop recording.
CI:> RECORD STOP ONTO SD00TEMP
- 5 This procedure is complete.

CallAgent RExTst minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
RExTst        .        .        ImgTst
```

Indication

The Call Agent generates a CCA660 log report to indicate that the RExTst started. The Call Agent generates a CCA661 to indicate that the RExTst finished and if the RExTst passed or failed.

Meaning

This alarm indicates a RExTst is in progress.

Action

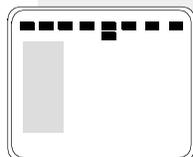
No action is required.

```
CallAgent      SYS      CON      APPL      Unit: 0
RExTst        .        .        .

Sys
0 Quit        Unit0  Inact  no       . Act   . Inact .   .   insync .
2 QryCPU      Unit1  Act    no       . Act   . Inact .   .   insync .
3 QryDsk
4 QryMem
5 QryZmb
6 QryNFS
7 QryLd
8 QryNTP
9 QryCpUtl
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh
   mtc
Time 14:56 >
```

Call Agent RExSch minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
RExSch        .        .        .
```

Indication

The Call Agent generates a CCA365 log report in addition to the alarm. The Call Agent generates a CCA665 log report when a Routine Exercise Test (REXTst) is run. Automatic scheduling of REXTsts is completed through table REXSCHED. Maintenance personnel may refer to a system initiated routine exercise test as an SREx Tst.

Meaning

A REXTst has not been run in the last seven days. Once a REXTst is run, the alarm clears. The REXTst must be a system initiated REXTst scheduled through table REXSCHED.

Action

At the MAP

- 1 Open IOAU112 log reports to determine if maintenance personnel have intentionally disabled REXTsts.

```
> LOGUTIL;OPEN IOAU112
```

- 2 Determine the next action.

| If REXTsts | Do |
|--------------------------------|-----------------------------|
| are intentionally disabled | This procedure is complete. |
| are not intentionally disabled | step 3 |

- 3 Enter table REXSCHED.

```
> QUIT ALL;TABLE REXSCHED
```

- 4 Use the POSITION and CHANGE commands to populate the table similar to the example.

```
TOP
      REXTSTID  ENABLE  PERIOD  PARALLEL
-----
      MS_REX_TEST      Y      1      1
      XACORE_REX_TEST  Y      1      1
      DAYSDBL
BOTTOM
>
```

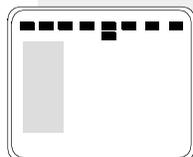
- 5 This procedure is complete.

Additional information

For more information about configuring system routine exercise tests, refer to table REXSCHED in *DMS-100 Customer Data Schema References Manual*, 297-8001-351 (NA) or 297-9051-351 (EMEA), and office parameter NODEREXCONTROL in *DMS-100 Office Parameters Reference Manual*, 297-8001-855 (NA) or 297-9051-855 (EMEA).

CallAgent simplex major

Alarm display



| | | | | |
|---------------------------|----------|--------------------|----------------------|---------|
| CallAgent simplex M | SYS . | CON MatCon M | APPL simplex M | Unit: 0 |
|---------------------------|----------|--------------------|----------------------|---------|

Indication

Since the mate Call Agent is unavailable, several CON and APPL alarms are generated. The Call Agent generates a CCA351 log report in addition to the alarm. The Call Agent generates a CCA651 log report when duplex operation is restored.

Status information for the mate unit is unavailable at the Call Agent Manager.

If a Call Agent card is locked by user action at the CS 2000 SAM21 Manager client, the Call Agent enters the locked-disabled-none state and appears with a hashed outline and a lock icon at the CS 2000 SAM21 Manager client. Duplex operation is restored after unlocking the card at the CS 2000 SAM21 Manager client and successful completion of application synchronization.

If a Call Agent card experiences a platform software error that prevents the Call Agent from providing service, the SAM21 Shelf Controller recovers the Call Agent. As the SAM21 Shelf Controller recovers the Call Agent, the Call Agent card icon appearance at the CS 2000 SAM21 Manager client changes. Refer to the introduction to this document and *SAM21 Shelf Controller Fault Management*, NN10089-911 for more information about SAM21 Shelf Controller automatic recovery.

Meaning

The mate Call Agent unit is unavailable.

Action

At the Call Agent Manager

- 1 Enter the CoreMtc level.

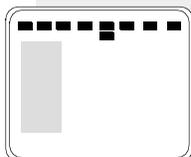
CoreMtc

```
CallAgent      SYS      CON      APPL      Unit: 1
  simplex      MatCon   simplex
  M            M
CoreMtc
0 Quit        Unit0  ----- state unavailable -----
2 CAMtc      Unit1  Act    no      . Act   . Inact S    S    nosync .
3 Sys
4 Con
5 Appl
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh
   mtc
Time 13:10 >
```

- 2 Check the following items to clear this alarm:
 - Mate Call Agent is in service
Check this at the CS 2000 SAM21 Manager client
 - Physical connections to the mate Call Agent are intact
- 3 This procedure is complete.

CallAgent C_MisM minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
C_MisM        .        .        .
```

Indication

The Call Agent generates log report CCA380 to indicate that the committed load mismatch alarm is raised. The Call Agent generates log report CCA680 to indicate that the alarm clears.

Note: This log report number was 372 and 672 in the SN04 and ISN04 releases.

Meaning

One Call Agent card has a different committed patch file version than the other card. This alarm clears when the same patch file version is committed on the second Call Agent card.

Action

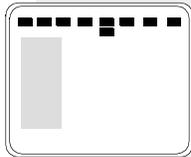
Commit the patch file on the second Call Agent card. Refer to the Patching software section of *Upgrading the Call Agent*, NN10065-461 for more information.

This alarm may appear temporarily during an upgrade while the two Call Agent cards have different patch files committed.

ATTENTION

Failure to correct a committed load mismatch alarm can result in the two Call Agent cards running different platform software versions in the event of an uncontrolled reboot.

Call Agent Config minor



CallAgent
Config

SYS
.

CON
.

APPL
.

Unit: 0

Indication

The Call Agent generates a CCA375 log report in addition to the alarm. The Call Agent generates a CCA675 log report once the alarm is cleared.

Meaning

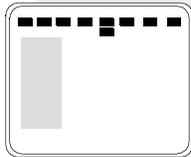
This alarm indicates that the two Call Agent cards are different card types with differences such as different processors. The alarm is expected during a Call Agent card upgrade and the alarm clears once the two Call Agent cards are of the same card type.

Action

No action is required.

CallAgent NIIKEY minor

Alarm display



```
CallAgent      SYS      CON      APPL      MC      Unit: 0  
NIIKEY        .        .        .        .
```

Indication

A CCA352 log report is generated when the alarm is raised. A CCA652 log report is generated when the alarm clears. This alarm is applicable to offices with Message Controllers only.

Meaning

This alarm indicates that a Network Filesystem (NFS) Inactive core Indicator Key (NIIKEY) file was detected in the /TAPE or /TAPE1 directory. If a call processing application restart occurs with the NIIKEY file present, the NIIKEY file prevents the call processing application from becoming the active instance.

The NIIKEY file is used by Nortel Installation Services personnel during a cutover procedure. If this alarm appears, contact Nortel support personnel.

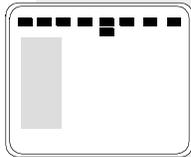
Action

Contact Nortel support personnel.

SYS CPU Ld

critical, major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              CPU Ld  .        .
```

Indication

The Call Agent generates a CCA301 log report in addition to the alarm. The Call Agent generates a CCA601 log report when the alarm clears.

Meaning

The CPU load average for one or more time segments has exceeded the threshold.

Action

At the Call Agent Manager

- 1 Enter the CoreMtc level.
CoreMtc
- 2 Enter the Sys level.
Sys

3 Check the CPU usage by issuing the QryCPU command.

```

CallAgent      SYS      CON      APPL      Unit: 0
.              CPU Ld   .        .

Sys
0 Quit         Unit0  Inact   no        . Act    . Inact  .      . insync .
2 QryCPU       Unit1  Act     no        . Act    . Inact  .      . insync .
3 QryDsk
4 QryMem
5 QryZmb
6 QryNFS
7 QryLd        CPU report retrieved on Tue Jul  2 13:28:50 2003:
8 QryNTP
9 QryCpUtl     1 min Load Avg: 5.25
10             5 min Load Avg: 3.01
11             15 min Load Avg: 2.95
12
13 LogQuery    Number of Processes: 52
14 Alarm
15 QueryIP     Alarm Description: 1 minute load average
16             Minor threshold: 10.00
17 Help        Major threshold: 20.00
18 Refresh     Critical threshold: 40.00
   mtc
Time 13:30 >

```

If

the alarm is critical

Do

Use the QryNFS command to determine if all mount points are accessible.

If some mount points are unavailable, use the DISKADM utility from the MAP to busy the missing volumes and troubleshoot STORM from the STORM Manager. Refer to *STORM Fault Management*, NN10088-911.

If all mount points are available, monitor call processing performance.

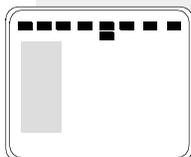
otherwise

Monitor the call processing performance. Refer to the *Call Agent Performance Management*, NN10153-711 for procedures.

4 This procedure is complete.

SYS Disk critical, major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              Disk    .        .
```

Indication

The Call Agent generates a CCA302 log report in addition to the alarm. The Call Agent generates a CCA602 log report when the alarm clears.

Meaning

The root file system for the Call Agent is a RAMDISK. Free space on the root file system is low. This alarm does not indicate that disk space on the STORAge Management (STORM) unit is low.

Note: Do not store files in the local file system.

Action

At the Call Agent Manager

- 1 Use the alarm sys command to determine which unit is alarmed.

Alarm Sys

```
SYS alarms for unit 0:
  Alarm Severity Description
  Disk critical Percentage of root free disk
                    space is less than or equal to
                    5.00; critical threshold
                    reached.
```

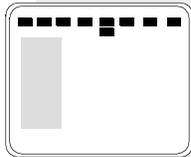
```
SYS alarms for unit 1: none
```

- 2 Contact Nortel support personnel.
- 3 This procedure is complete.

SYS Memory

critical, major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              Memory  .        .
```

Indication

The Call Agent generates a CCA300 log report in addition to the alarm. The Call Agent generates a CCA600 log report when the alarm clears.

Meaning

Free space in Random Access Memory (RAM) is low.

Action

At the Call Agent Manager

- 1 Enter the CoreMtc level.

CoreMtc

- 2 Enter the Sys level.

Sys

3 Check the memory usage by issuing the QryMem command.

```

CallAgent      SYS      CON      APPL      Unit: 0
.              Memory   .        .

Sys
0 Quit         Unit0  Inact   no       . Act   . Inact .   .   insync .
2 QryCPU      Unit1  Act     no       . Act   . Inact .   .   insync .
3 QryDsk
4 QryMem
5 QryZmb      Memory report retrieved on Wed Aug 27 09:07:45 2003:
6 QryNFS
7 QryLd       Total Memory: 986.54MB
8 QryNTP      Free Memory: 141.55MB
9 QryCpUtl    Cached Memory: 116.23MB
10           Shared Memory: 0.00MB
11           Buffer Memory: 0.78MB
12           Reserved Memory: 20.27MB
13 LogQuery   Available Memory: 238.29MB (free+cached+buffer-reserved)
14 Alarm
15 QueryIP    Alarm Description: Based on the amount of avail memory remain
16           Minor threshold: 150MB
17 Help       Major threshold: 125MB
18 Refresh    Critical threshold: 100MB
    mtc
Time 09:07 >

```

4 Determine the next action.

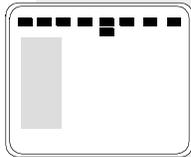
| If | Do |
|---|---|
| the alarm is minor severity | Record the alarm in office records. Monitor the system to determine if the problem escalates to major severity. |
| the alarm is major or critical severity | Contact Nortel support personnel. |

5 This procedure is complete.

SYS NFS

critical, major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              NFS      .        .
```

Indication

The Call Agent generates a CCA304 log report in addition to the alarm. The Call Agent generates a CCA604 log report when the alarm clears.

Meaning

One or more of the Network File System (NFS) mounted file systems is inaccessible. Each Call Agent mounts three file systems from each STORAGE Management (STORM) unit.

Action

At the Call Agent Manager

- 1 Enter the CoreMtc level.
CoreMtc
- 2 Enter the Sys level.
Sys
- 3 Check that no other alarms are masked by issuing the following command:
Alarm Sys

```
CallAgent      SYS      CON      APPL      Unit: 0
.              NFS      .        .
Sys
0 Quit
2 QryCPU      SYS alarms for unit 0:
3 QryDsk
4 QryMem      Alarm  Severity Description
5 QryZmb      NTP   minor  Host lost synchronization to one or more
6 QryNFS      servers; No. of configured server(s): 2; No.
7 QryLd      accessible server(s): 2; Host synchronized to:
8 QryNTP      1 server(s).
9 QryCpUtl
10           NFS   minor  Number of accessible mounts is between 1 and 5
11           minor threshold reached.
12
13 LogQuery   SYS alarms for unit 1:
14 Alarm
15 QueryIP    Alarm  Severity Description
16           NFS   minor  Number of accessible mounts is between 1 and 5
17 Help      minor threshold reached.
18 Refresh
   mtc
Time 19:05 >
```

Note: An NTP alarm was masked by the NFS alarm.

- 4** To determine the cause of the NFS alarm, issue the QryNFS command.

```

CallAgent      SYS      CON      APPL      Unit: 0
.              NFS      .        .

Sys
0 Quit         Unit0  Inact   no        . Act    . Inact  .      .   insync .
2 QryCPU      Unit1  Act     no        . Act    . Inact  .      .   insync .
3 QryDsk
4 QryMem      NFS mount report retrieved on Tue Jul  2 19:16:14 2002:
5 QryZmb
6 QryNFS      Number of accessible mounts: 3 / 6
7 QryLd
8 QryNTP      Local Name
9 QryCpUtl    /TAPE
10            /TAPE1
11            /3PC/sd00
12            /var/log
13 LogQuery   /var/log_mate
14 Alarm      /3PC/sd01
15 QueryIP
16            Alarm Description: Number of accessible mounts
17 Help      Minor threshold: 5
18 Refresh    Major threshold: 3
   mtc       Critical threshold: 2
Time 19:18 >

```

| Accessible |
|------------|
| Y |
| N |
| Y |
| N |
| Y |
| N |

- 5** Since half the mounts are inaccessible, check the following items as possible causes:

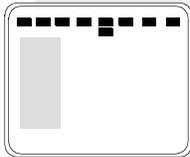
- STORM unit is out of service
Check this at the CS 2000 SAM21 Manager client or STORM Manager.
- STORM fiber channel connection is unplugged on STORM faceplate or Redundant Array of Inexpensive Disks (RAID) device
- STORM unit is misconfigured
Check this at the STORM Manager.

Refer to *STORM Fault Management*, NN10088-911.

- 6** This procedure is complete.

SYS NTP major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              NTP      .        .
```

Indication

The Call Agent generates a CCA305 log report in addition to the alarm. The Call Agent generates a CCA605 log report when the alarm clears.

Meaning

The platform software lost time synchronization to one or more Network Time Protocol (NTP) servers or the drift is excessive.

Action

At the Call Agent Manager

- 1 Enter the CoreMtc level.
CoreMtc
- 2 Enter the Sys level.
Sys

3 Check the NTP status by issuing the QryNTP command.

```

CallAgent      SYS      CON      APPL      Unit: 0
.              NTP      .        .

Sys
0 Quit         Unit0  Inact   no       . Act    . Inact  .      .   insync .
2 QryCPU      Unit1  Act     no       . Act    . Inact  .      .   insync .
3 QryDsk
4 QryMem
5 QryZmb
6 QryNFS
7 QryLd
8 QryNTP
9 QryCpUtl
10
11
12
13 LogQuery   NTP report retrieved on Tue Jul  2 20:24:22 2003:
14 Alarm
15 QueryIP    Total number of time servers: 2
16           Number of accessible servers: 2
17 Help      Number of synchronized servers: 1
18 Refresh   Time Offset from server 47.142.226.247: 6(ms)
   mtc
Time 20:25 >

```

4 To determine the NTP servers, exit the Call Agent Manager and check NTP provisioning on the Call Agent:

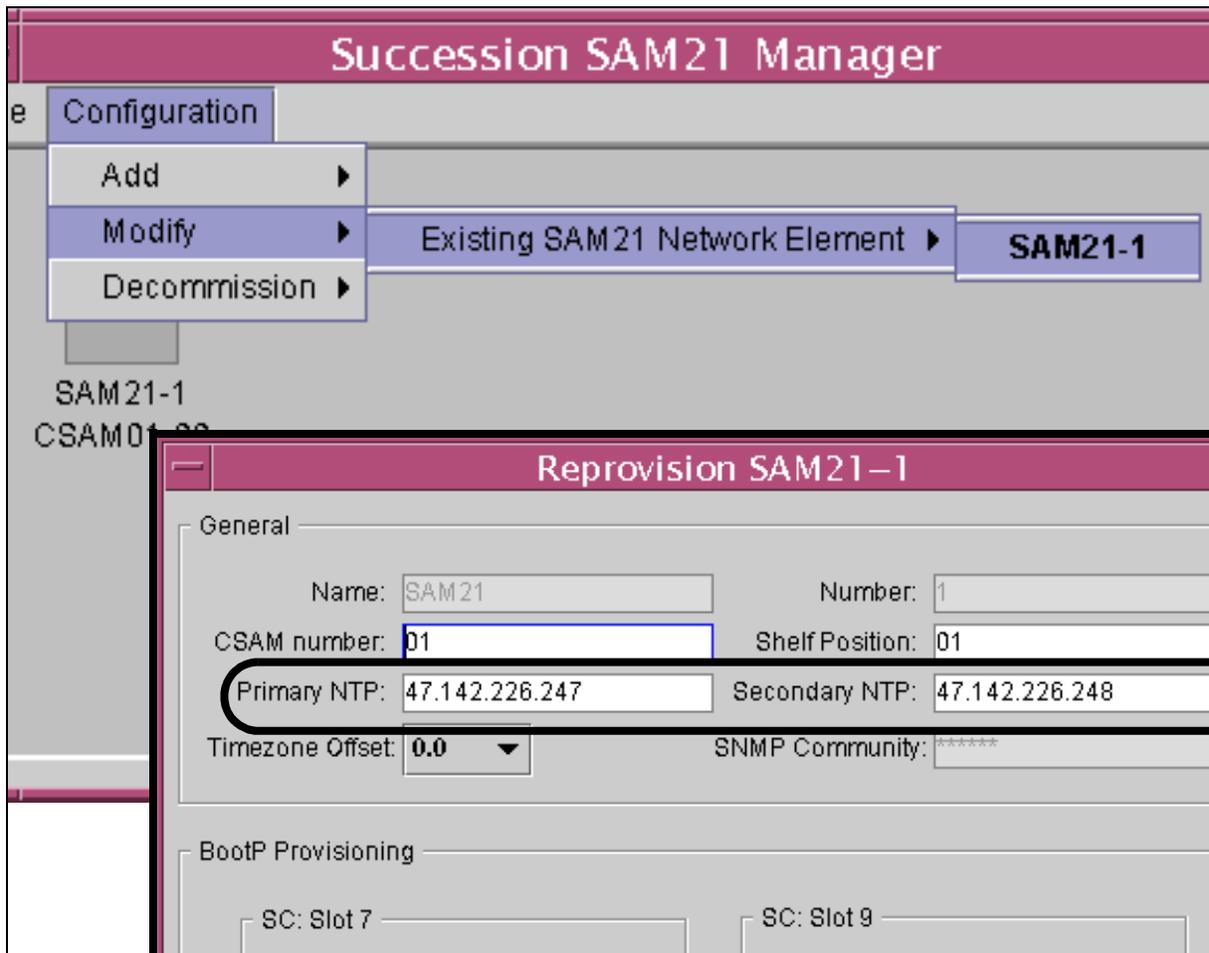
```
> 0 ALL
```

```
[mtc@ipaddress mtc]$ ntpq -n -p
```

The provisioned NTP information is displayed. Ensure that the IP addresses in the remote column match the NTP servers provisioned at the CS 2000 SAM21 Manager.

| remote | refid | st | t | when | poll | reach | delay | offset | jitter |
|-----------------|---------------|----|---|------|------|-------|-------|--------|--------|
| *47.142.226.247 | 47.129.242.21 | 3 | u | 31 | 64 | 377 | 1.637 | 6.550 | 0.413 |
| +47.142.226.248 | 47.129.242.23 | 4 | u | 40 | 64 | 377 | 0.687 | 6.549 | 0.712 |

5 Check provisioning from the CS 2000 SAM21 Manager client:



6 Determine next action.

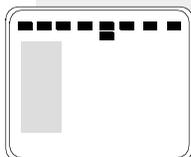
| If | Do |
|--|---|
| the time server is the CS 2000 Core Manager | Check the NTP service at the NTP level of sdmmtc. |
| primary and secondary server are the same server | Provision the Secondary NTP server to a new NTP server. |
| the time server is some other equipment | Refer to the product documentation. |

7 This procedure is complete.

SYS Zombie

critical, major or minor

Alarm display



| | | | | |
|-----------|--------|-----|------|---------|
| CallAgent | SYS | CON | APPL | Unit: 0 |
| . | Zombie | . | . | |

Indication

The Call Agent generates a CCA303 log report in addition to the alarm. The Call Agent generates a CCA603 log report when the alarm clears.

Meaning

One or more software process has terminated abnormally and may retain system resources such as memory space or CPU usage.

Action

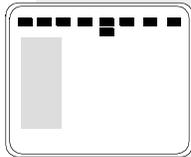
ATTENTION

Contact Nortel support personnel for assistance with zombie alarms. Failure to contact Nortel support personnel can result in a service interruption if system resources are consumed by many zombie processes.

SYS CpuUtl

critical, major or minor

Alarm display



| | | | | |
|-----------|--------|-----|------|---------|
| CallAgent | SYS | CON | APPL | Unit: 0 |
| . | CpuUtl | . | . | |

Indication

The Call Agent generates a CCA306 log report in addition to the alarm. The Call Agent generates a CCA606 log report when the alarm clears.

Meaning

The CPU utilization for one or more time segments has exceeded the threshold.

Action

At the Call Agent Manager

- 1 Enter the CoreMtc level.
CoreMtc
- 2 Enter the Sys level.
Sys

3 Check the CPU utilization by issuing the QryCpUtl command.

```

CallAgent      SYS      CON      APPL      Unit: 0
.              CpuUtl   .        .

Sys
0 Quit         Unit0   Inact   no      . Inact . Act   .      . insync .
2 QryCPU      Unit1   Act     no      . Inact . Act   .      . insync .
3 QryDsk
4 QryMem
5 QryZmb
6 QryNFS
7 QryLd
8 QryNTP
9 QryCpUtl
10             CPU Utilization report retrieved on Mon Mar 3 8:54:52 2003:
11
12             5 min Util Avg:100.00
13 LogQuery    20 min Util Avg: 89.83
14 Alarm       30 min Util Avg: 78.78
15 QueryIP     Alarm Description: cpu utilization average
16             Minor threshold: over 95.00% for 5 minutes
17 Help        Major threshold: over 99.00% for 20 minutes
18 Refresh     Critical threshold: over 99.00% for 30 minutes
   mtc
Time 8:55 >

```

If

the alarm is critical

Do

Use the QryNFS command to determine if all mount points are accessible.

If some mount points are unavailable, use the DISKADM utility from the MAP to busy the missing volumes and troubleshoot STORM from the STORM Manager client. Refer to *STORM Fault Management*, NN10088-911.

If all mount points are available, monitor call processing performance.

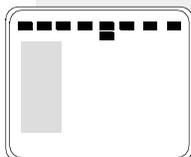
otherwise

Monitor the call processing performance. Refer to the *Call Agent Performance Management*, NN10153-711 for procedures.

4 This procedure is complete.

SYS HW Flt critical or major

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              HW Flt  .        .
               M
```

Indication

The Call Agent generates a CCA309 log report in addition to the alarm. The Call Agent generates a CCA609 log report when the alarm clears.

Meaning

The card has a Peripheral Component Interconnect (PCI) bus fault, Error Checking and Correction (ECC) memory fault, or a parity error.

Action

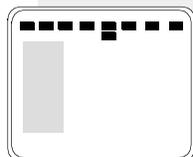
If the severity is minor, Lock the card, perform diagnostics, and Unlock the card to reset it. Refer to the Lock, diagnostics, and Unlock procedures in the *Call Agent Security and Administration*, NN10175-611.

If the severity is critical, replace the card. Refer to procedure [Replacing a Call Agent card on page 20](#).

This procedure is complete.

CON MatCon critical or major

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              .      MatCon  .
```

Indication

The Call Agent generates a CCA331 log report in addition to the alarm. The Call Agent generates a CCA631 log report when the alarm clears.

Meaning

A major severity alarm indicates that communication between the two Call Agent cards is unavailable over Ethernet or is unavailable over the fiber channel link. A critical severity alarm indicates communication between the two Call Agent cards is completely unavailable.

Investigate the following items when diagnosing this alarm:

- Ethernet link pull
- Fiber Channel pull
- CS LAN router misconfiguration
- inability to ping mate Call Agent from the active Call Agent
- inability to ping the active SAM21 Shelf Controller from the active Call Agent
- If the office has Message Controller cards, check for the ability to ping both Message Controller cards from the active Call Agent.

The description field of the MatCon alarm describes the connectivity map for the monitored connections. When Geographic Survivability is enabled, the description fields are extended to show enhanced connection monitoring. The fields are identical to the fields in logs CCA331 and CCA631. For description of the enhanced fields, refer to *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909.

Action

At the Call Agent Manager

- 1 View the alarms related to connectivity.

Alarm CON

Example system response:

```
CallAgent      SYS      CON      APPL      Unit: 0
.              .      MatCon  .
              C

CCAMtc
0 Quit
2 CoreMtc
3 Admin
4
5
6
7
8
9
10 CON alarms for unit 0:
11
12 Alarm Severity Description
13 LogQuery MatCon critical Link0: SYSB, mateCon UNAVAIL, netCon UNAVAIL;
14 Alarm      Link1: INSV, mateCon AVAIL, netCon AVAIL;
15            BLink: INSV, mateCon AVAIL;
16            FC: INSV;
17 Help      CON alarms for unit 1: none
18 Refresh
   mtc
Time 13:19 >
```

Example system response with Geographic Survivability enabled:

```
CallAgent      SYS      CON      APPL      Unit: 0
.              .      MatCon   .
              M

CCAMtc
0 Quit
2 CoreMtc
3 Admin
4 RExtTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh
   mtc
Time 13:19 >
```

```
CON alarms reported by CA unit 0:

Alarm Severity Description
MatCon major Link0: INSV, mateCon: OK (opt: BAD, wan: OK),
netCon: OK (local: OK, wanEdge: OK);
Link1: INSV, mateCon: OK (opt: BAD, wan: OK),
netCon: OK (local: OK, wanEdge: OK);
BLink: SYSB, mateCon: BAD;
FC: SYSB;
```

2 Use the following table to diagnose the mate connectivity alarm.

Mate connectivity alarm diagnosis

| If | Do |
|------------------------|---|
| Link0 or Link1 is MANB | Return to service the Ethernet link (RTSLnk) from the Con level of the Call Agent Manager. CoreMtc Con RTSLnk <0 or 1> |
| Link0 or Link1 is SYSB | <ul style="list-style-type: none"> • Verify that the Ethernet links are connected to the rear transition module of the SAM21 shelf. • Verify that the Ethernet links from the rear transition module of the SAM21 shelf connect to the router that provides the Communication Server Local Area Network (CS LAN). • Verify that the CS LAN router is in-service and that the ports are in-service. |
| FC is SYSB | <ul style="list-style-type: none"> • Verify that the mate Call Agent is in-service. • Verify that the fiber channel connection on the faceplate of each Call Agent is connected. |

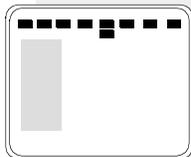
3 If Link0, Link1, and FC links are all restored to in-service (INSV) and the alarm persists, contact Nortel support personnel.

4 This procedure is complete.

CON LnkCon

critical or major

Alarm display



| | | | | |
|-----------|-----|--------|------|---------|
| CallAgent | SYS | CON | APPL | Unit: 0 |
| . | . | LnkCon | . | |
| | | M | | |

Indication

The Call Agent generates a CCA335 log report in addition to the alarm. The Call Agent generates a CCA635 log report when the alarm clears.

Meaning

A major severity alarm indicates that one of the Ethernet links is unavailable or the fiber channel is unavailable. A critical severity alarm indicates that both of the Ethernet links are unavailable.

If both Ethernet links are unavailable, the Call Agent reboots. Refer to [Network fault management strategy](#) for more information.

The description field of the LnkCon alarm describes the connectivity map for the monitored connections. When Geographic Survivability is enabled, the description fields are extended to show enhanced connection monitoring. The fields are identical to the fields in logs CCA335 and CCA635. For description of the enhanced fields, refer to *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909.

Action

At the Call Agent Manager

- 1 View the alarms related to connectivity.

Alarm CON

Example system response:

```

CallAgent      SYS      CON      APPL      Unit: 0
.              .        LnkCon    .
                M
CoreMtc        Jam:    Link0:    Link1:    BLink:    FC:    Appl:
0 Quit        Unit0  Act      no        . Act     S Inact  .      .    insync .
2 CAMtc       Unit1  Inact    no        . Act     . Inact  .      .    insync .
3 Sys
4 Con
5 Appl
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help        CON alarms for unit 1: none
18 Refresh
   mtc
Time 08:05 >

```

"S" indicates Link1 is system busy (SYSB)

```

CON alarms for unit 0:

Alarm Severity Description
LnkCon major Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
Link1: SYSB, mateCon: UNAVAIL, netCon: UNAVAIL;
BLink: INSV, mateCon: AVAIL;
FC: INSV

```

Example system response with Geographic Survivability enabled:

```

CallAgent      SYS      CON      APPL      Unit: 0
.              .      LnkCon   .
              M
CCAMtc
0 Quit         Unit0   Act   no   . Act   . Inact  Blnk:  FC:  Appl:
2 CoreMtc     Unit1   Inact no   . Act   . Inact  S      S      insync .
3 Admin
4 RExTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery    Alarm Severity Description
14 Alarm       LnkCon major Link0: INSV, mateCon: OK (opt: BAD, wan: OK),
15 QueryIP     netCon: OK (local: OK, wanEdge: OK);
16            Link1: INSV, mateCon: OK (opt: BAD, wan: OK),
17 Help        netCon: OK (local: OK, wanEdge: OK);
18 Refresh     BLink: SYSB, mateCon: BAD;
               FC: SYSB;
               mtc
Time 13:19 >

```

"S" indicates BLink and FC are system busy (SYSB)

CON alarms reported by CA unit 0:

Alarm Severity Description

LnkCon major Link0: INSV, mateCon: OK (opt: BAD, wan: OK),
netCon: OK (local: OK, wanEdge: OK);

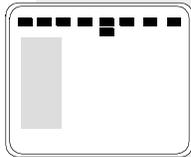
Link1: INSV, mateCon: OK (opt: BAD, wan: OK),
netCon: OK (local: OK, wanEdge: OK);

BLink: SYSB, mateCon: BAD;
FC: SYSB;

- 2** Verify Ethernet link connections. Follow the diagnostics in [step 2](#) of procedure [CON MatCon](#).
- 3** If the connectivity problem is with the fiber channel connection, BLink is SYSB and FC is SYSB. Verify that the fiber channel connection is intact at each Call Agent card and then begin diagnosing failures, faults, and misconfigurations with the optical transmission equipment between the two Call Agent units.
- 4** If link connectivity is restored and the alarm persists, contact Nortel support personnel.
- 5** This procedure is complete.

CON NetCon major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              .      NetCon  .
                M
```

Indication

The Call Agent generates a CCA336 log report in addition to the alarm. The Call Agent generates a CCA636 log report when the alarm clears.

Meaning

A minor severity alarm indicates that one Ethernet link does not have network connectivity. A major severity alarm indicates that both Ethernet links do not have network connectivity.

Note: In most circumstances, loss of both ethernet links causes the Call Agent to reboot. The major alarm may last only a short time because it is cleared when the Call Agent begins to reboot.

The description field of the NetCon alarm describes the connectivity map for the monitored connections. When Geographic Survivability is enabled, the description fields are extended to show enhanced connection monitoring. The fields are identical to the fields in logs CCA336 and CCA636. For description of the enhanced fields, refer to *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909.

Action

At the Call Agent Manager

- 1 View the alarms related to connectivity.

Alarm CON

Example system response:

```

CallAgent      SYS      CON      APPL      Unit: 0
.              .        NetCon    .
              m
CoreMtc
0 Quit         Unit0  Act     no      . Act   . Inact .   .   insync .
2 CAMtc       Unit1  Inact   no      . Act   . Inact .   .   insync .
3 Sys
4 Con
5 Appl
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help        CON alarms for unit 1: none
18 Refresh
   mtc
Time 08:13 >

```

```

CON alarms for unit 0:

Alarm Severity Description
NetCon minor   Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
Link1: INSV, mateCon: AVAIL, netCon: UNAVAIL;
BLink: INSV, mateCon: AVAIL;
FC: INSV;

```

Example system response with Geographic Survivability enabled:

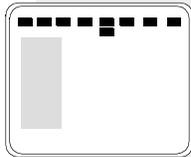
```
CallAgent      SYS      CON      APPL      Unit: 0
.              .      NetCon   .
              M

CCAMtc
0 Quit
2 CoreMtc
3 Admin
4 RExTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery    Alarm Severity Description
14 Alarm      NetCon major Link0: INSV, mateCon: OK (opt: OK, wan: OK),
15 QueryIP    netCon: OK (local: OK, wanEdge: BAD);
16           Link1: INSV, mateCon: OK (opt: OK, wan: OK),
17 Help      netCon: OK (local: OK, wanEdge: OK);
18 Refresh    BLink: SYSB, mateCon: OK;
           FC: SYSB;
           mtc
Time 13:19 >
```

- 2** Verify Ethernet link connections. Follow the diagnostics in [step 2](#) of procedure [CON MatCon](#).
- 3** If link connectivity is restored and the alarm persists, contact Nortel support personnel.
- 4** This procedure is complete.

APPL NoAppl critical or minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              .      .      NoAppl
```

Indication

The Call Agent generates a CCA316 log report in addition to the alarm. The Call Agent generates a CCA616 log report when the alarm clears.

Meaning

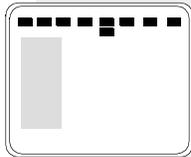
The call processing application software is booting or restarting. The alarm has minor severity if the alarm is raised against the inactive call processing application. The alarm has critical severity if the alarm is raised against the active call processing application.

Action

This alarm is raised during a transition state. No action is required.

APPL ImgTst minor

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              .              .              ImgTst
```

Indication

The Call Agent generates log report CCA620 during an image test. When the image test completes, the alarm clears and the Call Agent generates log report CCA621. CCA621 indicates if the test passed successfully or failed. If the test fails, the Call Agent generates a major image alarm (Image) and a CCA322 log report.

- CCA620 — image test started
- CCA621 — image test completed
- CCA322 — image test failed

Meaning

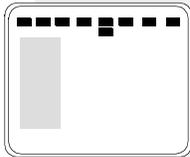
The inactive call processing application software is in test. This alarm is raised if the image test is manually run or if the image test is part of a manual or system routine exercise test (REXTst).

Action

No action is required.

APPL Image major

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              .              .      Image
                                   M
```

Indication

The Call Agent generates log report CCA322 in addition to the alarm. To clear the alarm, an image test is required. The results of the image test are indicated in a CCA621 log report.

Meaning

The inactive call processing application failed an image test.

Action

At the Call Agent Manager

- 1 Enter the image test query command at the application level.

```
CoreMtc
Appl
ImgTst QUERY
```

```
CallAgent      SYS      CON      APPL      Unit: 0
.              .        .        Image
              M
Appl
0 Quit         Unit0   Act     no      . Inact . Act   .   .   insync .
2 ImgTst      Unit1   Inact   no      . Inact . Act   .   .   insync .
3 Sync
4 DpSync
5
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP     Last run on: Thu Apr 10 13:17:57 2003
16            CA Unit Tested: 1
17 Help       Restart Type: ALL
18 Refresh    Result: FAILED
mtc
Time 10:03 >
```

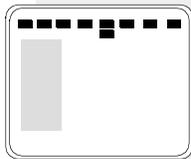
- 2 Record the results in office records.

| If | Do |
|--|---|
| office records indicate that the fault has occurred before | Contact Nortel support personnel. |
| there is no record of a previous image test failure | Run a manual image test. Refer to <i>Call Agent Security and Administration</i> , NN10175-611 for information on running image tests. |
| | If the test fails again, contact Nortel support personnel. |

- 3 This procedure is complete.

APPL simplex major

Alarm display



```
CallAgent      SYS      CON      APPL      Unit: 0
.              .      .      simplex
               .      .      M
```

Indication

The Call Agent generates log report CCA315 in addition to the alarm. The Call Agent generates log report CCA615 when the alarm clears.

Meaning

The inactive call processing application is not ready for takeover without an outage. Possible reasons for raising this alarm are listed:

- If the mate Call Agent is out of service, this alarm is raised with a CallAgent simplex alarm and additional alarms. Clear the CallAgent simplex alarm first. A switch of activity will not occur under this condition.
- If the fiber channel connection to the mate is unavailable, this alarm is raised with a minor MatCon alarm. Clear the MatCon alarm first. A switch of activity can occur under this condition and the newly active Call Agent will trigger a restart reload. A restart reload indicates a complete loss of call processing during the restart and all calls are dropped.

If the APPL simplex alarm persists and a switch of activity does occur, any provisioning or operational data changes that occurred after the loss of synchronization are lost.

Action

At the Call Agent Manager

- 1 Enter the maintenance level and verify that the mate Call Agent is in-service (INSV).

CoreMtc

```

CallAgent      SYS      CON      APPL      Unit: 0
.              .              .              simplx
              M
CoreMtc
0 Quit        Unit0 Act    no    . Inact . Act    .    .    nosync .
2 CAMtc      Unit1 Inact  no    . Inact . Act    .    .    nosync .
3 Sys

```

If one of the circled units indicates “state unavailable,” then the mate Call Agent is unavailable. Follow to the taskflow in [Fault management taskflow on page 7](#) of this document for diagnostics.

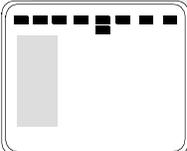
- 2 Enter the application level and synchronize the call processing application.

Appl Sync

- 3 Contact Nortel support personnel if the alarm persists.
- 4 This procedure is complete.

APPL Memory major or minor

Alarm display



| | | | | |
|-----------|-----|-----|----------------|---------|
| CallAgent | SYS | CON | APPL Memory | Unit: 0 |
| . | . | . | | |

Indication

The Call Agent generates a CCA314 log report in addition to the alarm. The Call Agent generates a CCA614 log report when the alarm clears.

Meaning

Free space in the Data Store (DS) area of memory for the call processing application is below a threshold. The threshold is 48 megabytes for minor severity and 32 megabytes for major severity.

When the Call Agent boots, the operating system allocates memory for the call processing application. The call processing application then applies its own memory management within the allocated memory. This alarm indicates that free space in the allocated memory is low.

Because the alarm relates to the memory allocated to the call processing application, this alarm is similar, but unrelated to the SYS Memory alarm.

The call processing application audits memory usage during every image test. A platform software process initiates a memory audit every five minutes unless a maintenance process is in progress.

Action

Contact Nortel support personnel immediately.

For minor severity alarms, no new datafill should be performed to the application image until the problem is understood and a plan is in place. Proceeding with further datafill will reduce the amount of memory available and the alarm will progress to a major.

For major severity alarms, stop all datafill and use of system tools. Limit system activities to critical issues only. Contact Nortel support personnel immediately as a future upgrade is at risk of failure.

MAP alarm clearing procedures

The call processing application provides the MAP.

Fault management assistance is provided from the maintenance (MTC) level of the MAP.

```
CI:
>MAPCI ; MTC
```

MTC level

The MTC level provides an alarm banner for troubleshooting assistance.

```

      IOD          CCS      Lns      Trks      Ext      APPL
      .            .        .        .        .        .

MTC
0 Quit          MTC:
2 Activity
3
4 SRSTATUS
5 BERP
6 CAPACITY
7
8
9
10
11 IOD
12
13
14 CCS
15 Lns
16 Trks
17
18 APPL
  USERNAME
Time 16:03 >
```

A dot indicates that services are operating normally.

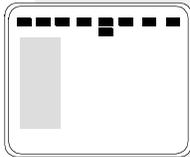
If an alarm appears, the dot is replaced with an abbreviation for the alarmed subsystem. Below the abbreviation, "M" indicates a major alarm and "C" indicates a critical alarm. Otherwise, the alarm is of minor severity.

- Input/Output Device (IOD) alarms are cleared from the IOD level.
- Common Channel Signaling (CCS) alarms are cleared from the Universal Signaling Point (USP) or CS 2000 USP - Compact Manager client.
- Line (Lns) alarms are cleared from the Lines Maintenance Manager (LMM).

- Trunk (Trks) alarms are cleared from the Trunks Maintenance Manager (TMM).
- External alarm system (Ext) alarms are cleared from the Ext level.
- Application (APPL) alarms are cleared from the APPL level.

APPL alarms critical, major or minor

Alarm display



```

IOD          CCS      Lns      Trks      Ext      APPL
.            .        .        .        .        xxxxxxx
  
```

Additional information

Several alarms under the application (APPL) level of the MAP are related to the SuperNode Billing Application (SBA). Refer to the *CS 2000 Core Manager*, NN10082-911 for clearing the following SBA related alarms:

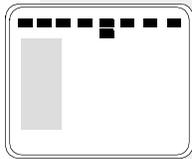
| | | |
|--------|--------|--------|
| BACK50 | FTPW | NOREC |
| BACK70 | LODSK | NOSTOR |
| BACK90 | NOBAK | NOVOL |
| BACKUP | NOCLNT | SBACP |
| DISKWR | NOCOM | SBAIF |
| FTP | NOFL | |

Note: Many SBA alarm clearing procedures refer to CM, XACORE, SLM, and disk volumes that begin with S00D. Refer to the following chart for a cross reference.

| SBA reference | Use |
|---|------------------------------|
| CM, XACORE | Call Agent |
| SLM | STORage Manager (STORM) |
| S00D<volume>, S01D<volume>, F02L<volume>, F17U<volume> | SD00<volume> or SD01<volume> |

IOD ITOC major or critical

Alarm display



| IOD | CCS | Lns | Trks | Ext | APPL |
|------|-----|-----|------|-----|------|
| ITOC | . | . | . | . | . |
| *C* | | | | | |

Indication

At the MTC level of the MAP display, ITOC appears under the Input/Output Devices (IOD) header of the alarm banner. The ITOC indicates an image table of contents (ITOC) critical alarm.

Meaning

Image files are not registered or do not exist in the computing module (CM) ITOCs. If the CS 2000 - Compact is configured with Message Controller cards, this alarm is also raised when an image file is not registered in the ITOC for the Message Switch (MS).

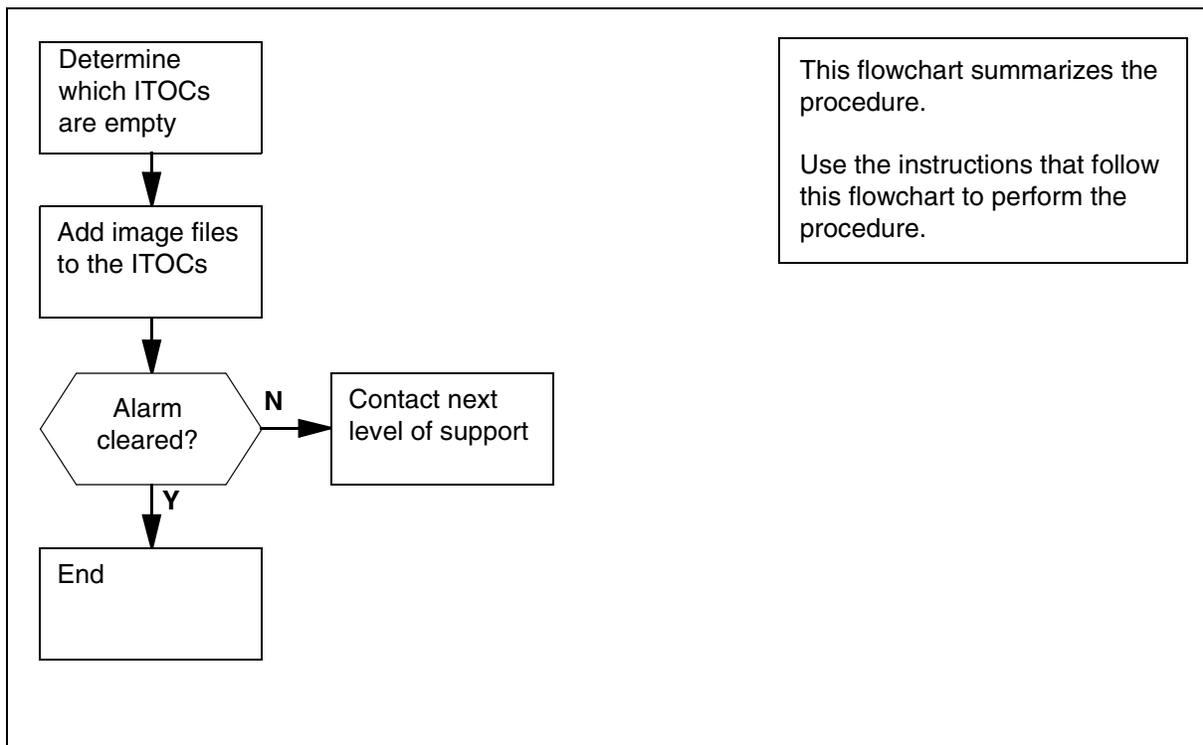
Result

A reload initiated during an ITOC critical alarm can cause a loss of service.

Action

The following flowchart is a summary of the procedure. Use the instructions in the procedure that follows the flowchart to clear the alarm.

Summary of clearing an IOD ITOC critical alarm



At the MAP

- 1 Ensure that you are at the CI level of the MAP display.
>QUIT ALL
- 2 Access the disk utility.
>DISKUT
- 3 List the volumes.
>LV

```

>LV
Volumes found:
-----
NAME                TYPE      TOTAL    FREE TOTAL  OPEN  ITOC    LARGEST
                   BLOCKS   BLOCKS  FILES  FILES  FILES  FREE
-----
SD00SBA             STD      819200      0    130    0      0
SD00IMAGE           STD     1638400    855040    1      0      1  855040
...
SD01IMAGE           STD     1638400    814430    3      0      0  814430
SD01PERM            STD     262144    262144    0      0      0  262144
SD01TEMP            STD     262144    262134    1      0      0  262134
Total number of volumes listed: 35.
>

```

- 4 Determine from office records the volumes that contain the image files (one image volume for each storage device).
- 5 List the file information for the image volumes.

```
>LF volume_name
```

volume_name

is the name of the volume that contains the image files

```

>LF SD01IMAGE
File information for volume SD01IMAGE:
{NOTE: 1 BLOCK = 512 BYTES }
-----
FILE NAME                O R I O O V FILE  MAX  NUM OF  FILE  LAST
                          R E T P L L CODE  REC  RECORDS  SIZE  MODIFY
                          G C O E D D      LEN  IN      IN  DATE
                          C N          FILE  BLOCKS
-----
.ITOC                     O F          0  1024      1      2  020309
CSNW04AY                  I F          0  1020    202152  402725  020103

```

- 6 Determine if a registered image file exists in the ITOC.

Note: The letter Y under the ITOC header confirms the file in the ITOC is registered. The area is blank if a registered file does not exist. The MAP response in step 5 does not contain an image file in the ITOC. If the office is configured with Message Controllers, ensure that an entry for the Message Switch is set to Y too.

If a CM image file

Do

is registered

step [11](#)

is not registered

step [8](#)

- | | If a CM image file | Do |
|----------|--|------------------------|
| | does not exist | step 7 |
| 7 | Use the AUTODUMP utility to take an image. >AUTODUMP MANUAL Note: If table IMAGEDEV is not provisioned, use the table editor to enter a volume name and activate the volume. | |
| 8 | Record the file name of the current image file. Note: In the MAP response in step 5 , the current image file is CSNW04AY. | |
| 9 | Enter the ITOCCI level and add the current image file to the ITOC. >ITOCCI; SBF CM file_name 1 ALR file_name is the name of the current image file Note: Use the SBF MS command for the MS. | |

```

>SBF CM CSNW04AY 1 ALR
CSNW04AY is registered in CM ITOC.
The updated ITOC is listed directly below.
Image Table Of Contents:
  A Registered          Generic Device          File
  L Date                Time                    Name
  R MM/DD/YYYY HH:MM:SS
-----
  0  03/09/2002 13:02:35 SD00IMAGE             PSNNCSH04BG_CM
  1 * 03/09/2002 13:36:56 SD01IMAGE             CSNW04AY
>

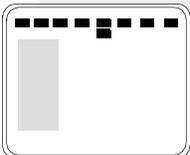
```

- 10** Determine if the ITOC critical alarm cleared.

- | | If the alarm | Do |
|-----------|-----------------------------------|-------------------------|
| | cleared | step 12 |
| | did not clear | step 11 |
| 11 | Contact Nortel support personnel. | |
| 12 | The procedure is complete. | |

IOD DISK major or critical

Alarm display



| IOD | CCS | Lns | Trks | Ext | APPL |
|------|-----|-----|------|-----|------|
| DISK | . | . | . | . | . |
| *C* | | | | | |

Indication

At the MTC level of the MAP display, DISK appears under the Input/Output Devices (IOD) header in the alarm banner.

The call processing application also generates a DISK650 log report to indicate that the disk availability audit failed.

A DISK530 log report indicates that maintenance personnel manually busied (MANB) a volume. When volumes are returned to service, manually or through software processes, a DISK520 log report indicates that the volume is available.

Meaning

This alarm indicates that the call processing application cannot access one or more disk devices (SD00 or SD01) or that volumes on a disk device are unavailable (SD00AMA).

A critical level alarm indicates that both disk devices are inaccessible. A major level alarm indicates that one disk device has accessible volumes. A minor level alarm indicates that both disk devices are accessible, but one or more volumes on a disk device are inaccessible.

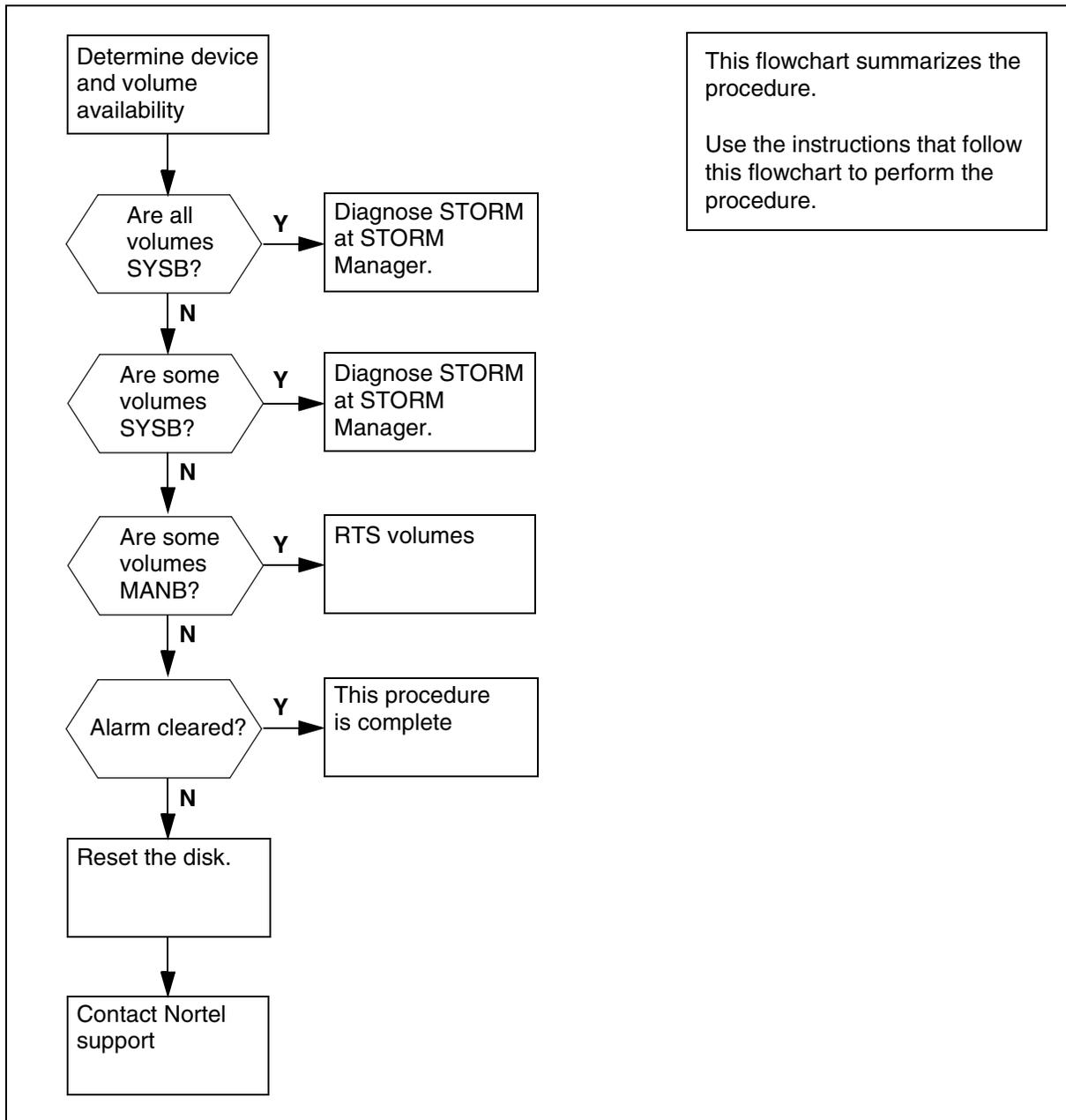
Result

If access to both disk devices fail, Device Independent Recording Package (DIRP) subsystems can backup to memory and consume memory space.

Action

Review the following flowchart for an overview of the alarm clearing procedure. Perform the procedure that follows the flowchart.

Summary of clearing an IOD DISK alarm



At the MAP

- 1 Enter the disk administration level and display the volumes for both disk devices.

```
>DISKADM SD00; DV; QUIT
```

```
>DISKADM SD01; DV; QUIT
```

2 Determine the device and volume availability.

Information about disk volumes on device SD01.

| Volume Name And State | Create Date Y/M/D | Modify Date Y/M/D | Size Mega- bytes | Vol. No. | ITOC Files | Volume Path |
|-----------------------|----------------------|----------------------|------------------------|----------|------------|-------------------|
| SBA | S 2002/04/15 | 2002/07/04 | 1024 | 0 | 0 | /3PC/sd01/sba/ |
| DLG0 | S 2002/05/01 | 2002/07/17 | 63 | 1 | 0 | /3PC/sd01/dlg0/ |
| IMAGE0 | S 2002/04/15 | 2002/06/26 | 1024 | 2 | 0 | /3PC/sd01/image0/ |
| DLG1 | S 2002/05/01 | 2002/07/17 | 63 | 3 | 0 | /3PC/sd01/dlg1/ |
| IMAGE1 | S 2002/05/01 | 2002/07/04 | 1024 | 4 | 0 | /3PC/sd01/image1/ |
| DLG2 | S 2002/05/01 | 2002/07/18 | 63 | 5 | 0 | /3PC/sd01/dlg2/ |
| DLG3 | S 2002/05/01 | 2002/07/18 | 63 | 6 | 0 | /3PC/sd01/dlg3/ |

S indicates system busy (SYSB)
M indicates manual busy (MANB)
. indicates in-service (INSV)

| If | Do |
|--|--|
| all volumes on a disk device (SD00 or SD01) are SYSB | Use the CS 2000 SAM21 Manager to determine if the STORM cards are unlocked-disabled or alarmed. Refer to Card icons for assistance with diagnosing the STORM card states. If a STORM card is unlocked-disabled or alarmed, lock and unlock the card. If the STORM cards are unlocked-enabled and in-service, use the STORM Manager to determine if there are any connectivity or fiber channel faults to the Redundant Array of Inexpensive Disks (RAID) device. |
| some volumes on a disk device are SYSB | Use the STORM Manager to determine if there are connectivity faults to the RAID device or if exported file systems have been removed. |
| some volumes are MANB | Use the RTS ALL command to restore the devices. |

- 3 If the DISK alarm does not clear, use the RESETDISK command.
> BSY ALL;RESETDISK;RTS ALL
- 4 If the DISK alarm does not clear, contact Nortel support personnel.
- 5 This procedure is complete.

Additional information

Refer to the following figure for examples of DISK log reports.

```
OFC_NAME      DISK530 JUL30 09:58:27 9900 MANB Volume MBSY
NAME: SD00ADUMP1
DESCRIPTION: Disk volume is no longer available.
```

```
OFC_NAME      DISK520 JUL30 10:01:33 4600 RTS  Volume RTS
NAME: SD01DLGP
DESCRIPTION: Disk volume is now available.
```

```
OFC_NAME      DISK650 JUL30 10:06:12 6400 INFO
NAME: SD01
DESCRIPTION: Audit Test Failed
```

```
Recovery audit failed (22): #001D 003D.
```

Creating a test volume on a disk

Application

Use this procedure to create a test volume on a disk.

The tests make sure that the communication with the STORAge Management (STORM) devices is intact.

Interval

Perform this procedure after installation of a new disk in a STORM unit, a reboot of a STORM unit, and after a STORM upgrade. If performing this procedure after a disk replacement in a STORM unit, wait for the unit to rebuild the array. Array rebuild status is available at the Storage panel of the STORM Manager.

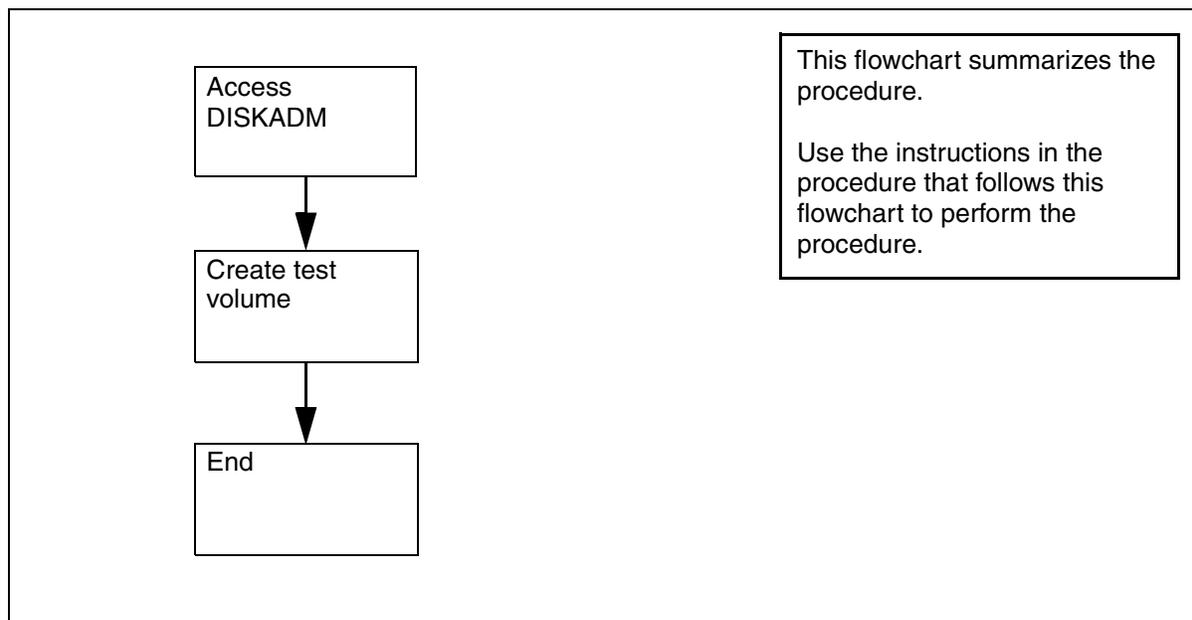
Common procedures

There are no common procedures.

Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

Creating a test volume



At the MAP

- 1 Access the disk administration level:

```
>DISKADM SD<nn>
```

nn
is 00 or 01

```
>DISKADM SD00
DISKADM
Administration of device SD00 (0) is now active.
>
```

- 2 Display the disk space that is available:

```
>DD
```

```
>DD
Disk drive information for SD00 (0):
Number of volumes in service           : 15 of 15
Total space for volumes                 : 7992 Mbytes
Total volume space allocated           : 3704 Mbytes
Remaining free space for new volumes   : 3951 Mbytes
Composite free space reported by device : 5712 Mbytes
Device communication:                  : Okay
1 Mbyte = 1024*1024 bytes.
>
```

- 3 Create a test volume on the disk:

```
>CV <name> <size>
```

name

is a character string that of 16 or fewer characters

size

is an integer value between 16 and 16 384 and indicates the size of the volume in megabytes

```
>CV TSTVOL 128
Created volume TSTVOL (15) successfully.
Enabled volume TSTVOL (15) successfully.
Creation of the volume TSTVOL is completed on device SD00.
>
```

- 4 Quit the DISKADM utility:

```
>QUIT
```

5 This procedure is complete.

Additional information.

To delete the volume, use the **DDV** command in DISKADM.

Recording an office image on a disk

Application

Use this procedure to record the office image to a disk.

Interval

Perform this procedure each day if automatic image taking is not configured. Perform this procedure as required by your office if automatic image taking is configured.

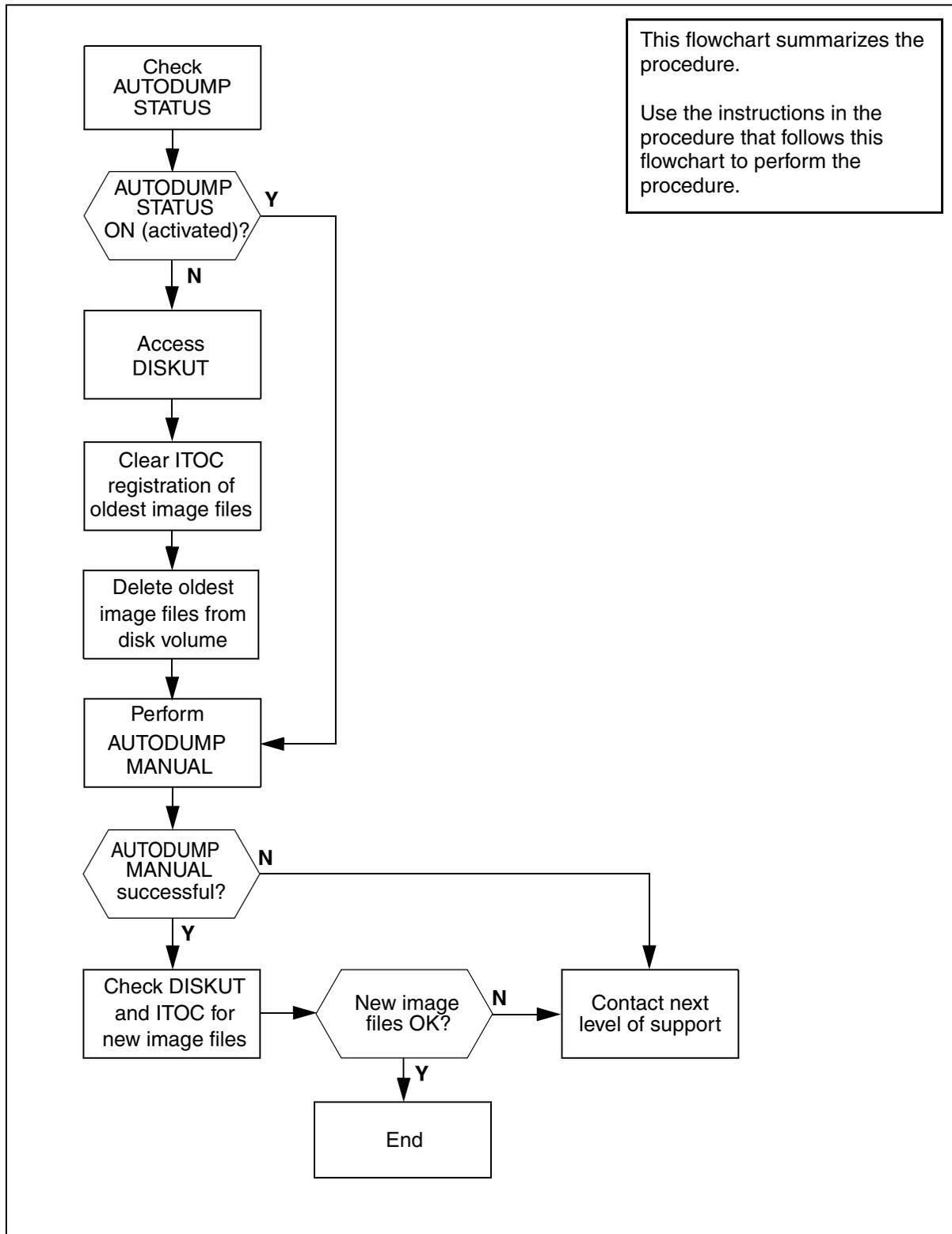
Common procedures

There are no common procedures.

Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

Summary of recording an office image on a disk



At the MAP

- 1 Access the CI level:
> **QUIT ALL**
- 2 Check the status of automatic image taking:
> **AUTODUMP STATUS**

Example of a MAP response

```
No Successful Image Information Available.  
  
No Last Image Information Available.  
  
SCHEDULED-Image Dump is ON.  
  
RETAIN option is OFF.  
  
Next scheduled dump is MONDAY at 21:00 hours.  
Next image to be dumped on SD00IMAGE1.  
>
```

- 3 Determine if the retain option is off. In the example of a MAP response of [step 2](#), the text `RETAIN option is OFF` indicates the retain option is off.

| If RETAIN option is | Do |
|---------------------|------------------------|
| ON | step 4 |
| OFF | step 5 |

- 4 To change the retain option, type:
> **AUTODUMP RETAIN**

The command requires a confirmation. Confirm the prompt with a 'Y.' Example of a MAP response:

```
RETAIN option is currently ENABLED.
The PRIMARY LOAD ROUTE should be currently
set per NTP.
Please refer to NTP before disabling.
The RETAIN option will be DISABLED.
Please confirm ("YES", "Y", "NO", "N"):
>Y
RETAIN option DISABLED.
>
```

- 5 Determine if automatic image taking on or off. In the example of a MAP response of [step 2](#), the text SCHEDULED-Image Dump is ON indicates the automatic image taking is on.

| If SCHEDULED-Image Dump is | Do |
|----------------------------|-------------------------|
| ON | step 19 |
| OFF | step 6 |

- 6 Access the MAP disk utility:
- ```
> DISKUT
```
- 7 Determine and record the disk volume to use for recording image dumps. Determine the disk volume from office records or office personnel.
- 8 To list the files in the disk volume that you recorded in [step 7](#), type:
- ```
> LISTFL <volume_name>
volume_name
is a volume name like SD00IMAGE1
```

Example of a MAP response:

```
>LF SD00IMAGE1
```

```
File information for volume SD00IMAGE1:
```

```
{NOTE: 1 BLOCK = 512 BYTES }
```

```
-----
FILE NAME                O R I O O V FILE  MAX   NUM OF   FILE   LAST
                        R E T P L L CODE  REC   RECORDS  SIZE  MODIFY
                        G C O E D D   LEN     IN     IN    DATE
                        C N                FILE  BLOCKS
-----
CSNW06BU_P0726V3_CM     I F Y             0 1020   212293 422928 030730
CSNW06CD_P0806_CM       I F Y             0 1020   212358 423057 030806
.ITOC                   O F               0 1024     1     2 030917
CSNW06CD_CM             I F Y             0 1020   212358 423057 030731
CSNW06CD_P0813_CM      I F Y             0 1020   212423 423187 030813
-----
```

- 9 Determine and record the file names of the oldest CM image and message switch (MS) image. The image files have a CM suffix. The MS image files have an MS suffix.

Note: In the example of a MAP response in [step 8](#), the oldest image file is CSNW06BU_P0726V3_CM. In the example of a MAP response in [step 8](#), there is no example for a MS image.

- 10 Determine if you can delete the files of the oldest image and MS image. Determine if file deletion is correct from office records or office personnel.

If file deletion of oldest CM image and MS image is **Do**

correct

[step 11](#)

not correct

Contact your next level of support.

- 11 Access the user interface for the image table of contents (ITOC) table:

```
> ITOCCI
```

12

**WARNING****Do not leave ITOC table empty**

The ITOC table must not be empty of image files to boot the switch. Do not clear all CM and MS image files from the ITOC.

List the CM image files in the ITOC:

> **LISTBOOTFILE CM**

Example of a MAP response:

Image Table Of Contents:

| A | Registered | | Generic Device | File |
|---|------------|------------|----------------|--------------------------------|
| L | Date | Time | | Name |
| R | MM/DD/YYYY | HH:MM:SS | | |
| 0 | * | 08/13/2003 | 21:12:49 | SD00IMAGE1 CSNW06CD_P0813_CM |
| 1 | | 07/31/2003 | 22:48:39 | SD00IMAGE1 CSNW06CD_CM |
| 2 | | 07/30/2003 | 04:12:34 | SD00IMAGE1 CSNW06BU_P0726V3_CM |
| 3 | | 08/06/2003 | 21:31:02 | SD00IMAGE1 CSNW06CD_P0806_CM |

Note: The example of a MAP response identifies the autoload registered (ALR) image file by an asterisk (*) in the ALR column. Each image file has an index number at the beginning of the tuple line. The ALR image in the example of a MAP response has an index number of 0. The ALR image file is selected first to boot the switch. If the ALR image file does not boot the switch then image file with the next index number is used.

13 Determine if the ITOC table has more than one CM image file.

If more than one CM image file is **Do**

in the ITOC table

[step 14](#)

not in the ITOC table

Contact your next level of support.

14 Clear the oldest image file from the ITOC table:

> **CLEARBOOTFILE CM FILE <cm_image_file>**

cm_image_file

is the name of the image file recorded in [step 9](#)

Example

> **CBF CM FILE CSNW06BU_P0726V3_CM**

15 If necessary, clear the oldest MS load just as for the CM:

> **LISTBOOTFILE MS**

> **CLEARBOOTFILE MS FILE <ms_image_file>**

16 Quit the ITOCCI level:

> **QUIT**

17 Delete the image files removed from the ITOC:

> **DELETEFL <cm_image_file>**

> **DELETEFL <ms_image_file>**

The DELETEFL command requires confirmation of the command. Confirm the prompt with a 'Y.'

18 Quit the disk utility level:

> **QUIT**

19 Start recording the image:

> **AUTODUMP MANUAL**

Example of a MAP response:

```
> AUTODUMP MANUAL
13:19 SCHEDULED Image Dump in approximately 5 minutes...
13:19 Using enhanced checksum check method ...
13:19 Please refrain from using dump unsafe commands during the CM image
13:19 Quit to CI if possible.
13:19 If you cannot refrain from using dump unsafe commands
13:19 use the STOPDUMP command to abort AUTODUMP.
13:19 Checking to see if anyone is using dump unsafe commands.
13:19 There are no users of dump unsafe commands.
>
13:22 SCHEDULED Image Dump in 2 minutes...
13:22 Use STOPDUMP command to ABORT.
13:22 Checking to see if anyone is using dump unsafe commands.
13:22 There are no users of dump unsafe commands.
13:24 Starting SCHEDULED Image Dump.
13:24 Checking to see if anyone is using dump unsafe commands.
13:24 There are no users of dump unsafe commands.
13:24 Querying image size on node: CM. Waiting for reply...
13:24 Reply received.
13:24 Checking to see if anyone using dump unsafe commands.
13:24 There are no users of dump unsafe commands.
13:24 Image Dump STARTED: 2003/09/29 13:24:08.257 MON.
13:24 Please refrain from using dump unsafe commands during the CM image
13:24 Quit to CI if possible.
13:24 If you cannot refrain from using dump unsafe commands
13:24 use the STOPDUMP command to abort AUTODUMP.
13:24 Users will be notified when dump unsafe commands are allowed to be
13:24 A CM image dump is starting.
13:24 Commands set to NOTSAFE or PS in table CMDS cannot be used.
13:25 Recent change commands (PS dump safe) can be entered now.
13:27 Image dump completed successfully.
```

20 Check the performance of the image taking record of [step 19](#):

>AUTODUMP HISTORY

Example of a MAP response:

AUTODUMP HISTORY example

```
> AUTODUMP HISTORY
Successful Image: S030929132424_CM
Taken: 2003/09/29 13:24:08.257 MON.
On Volume: SD00IMAGE1

Last Image: S030929132424_CM
Taken: 2003/09/29 13:24:08.257 MON.
On Volume: SD00IMAGE1

Printing History File for Last Image...
Autodump begins...

Stopping Journal File...
Journal File stopped.

Beginning Dump. START time: 2003/09/29 13:24:08.261 MON.
Timeout initialized.
CM: The Checksum Check method will be used for this image dump.
CM: Unloading modules that are loaded as TEMPORARY...
CM: None found.
CM: Old autoload file: SD00IMAGE1 CSNW06CD_P0813_CM
CM: Estimated image size is 205923 Kbytes.
CM:
CM:
CM: Dumping Data Store.
CM: DS dump time 94836 records was 00:01:34
CM:
CM: Checking Data Store.
CM: DS check time was 00:00:02
CM:

Rotating Journal File...
Rotate Initiated. Check DIRP log for details.

Starting Journal File...
Failed to START Journal File.
CM:
CM: Dumping Program Store.
CM: PS dump time 111086 records was 00:01:50
```

```

CM:
CM: Dumping Entry Record.
CM:
CM: Checking Program Store.
CM: PS check time was 00:00:02
CM:
CM: Checking Entry Record.
CM:
CM: Successful DUMP and CHECK.
CM: 205923 blocks with 3446 corrections.
CM:
CM: Image from CM registered as file 15 in ITOC for CM.
CM: Active entry in ITOC for CM was updated.
Image Dump Completed.
Dump END time: 2003/09/29 13:27:44.215 MON..

Renaming CM Image File from ACTIVE to SAFE:
CM Image File Renamed.

Store Usage:
DS:  USED = 231003Kb  AVAIL = 4069Kb  TOTAL = 235072Kb  % USED = 98%
PS:  USED = 107494Kb  AVAIL = 1882Kb  TOTAL = 109376Kb  % USED = 98%
Autodump ends...

```

- 21** Determine if the image taking record completed correctly.
- | If image taking completed | Do |
|---------------------------|-------------------------|
| correctly | step 23 |
| not correctly | step 22 |
- 22** Find additional information about the error and contact the next level of support:
- > **AUTODUMP DEBUG**
- 23** Access ITOCCI and verify that the images for CM and MS are set to ALR:
- >**ITOC CI; LBF CM; LBF MS**
- The ITOC is displayed. Verify that the ITOC was updated, and that the latest images are set to ALR.*
- 24** You have completed this procedure. If telephone operating company policy requires a backup to tape, perform that procedure now.

Restoring a Call Agent

This procedure describes how to restore an archived call processing application image from tape.



CAUTION

Possible service interruption

Do not use this procedure when in an emergency situation with no stable call processing application image.

If in a situation without a restartable image, contact Nortel Global Network Product Support (GNPS) immediate. Attempting to use this method without a valid call processing application image could fail due to constant resets on the Call Agent.

At the SDM

- 1 Insert the DAT cassette with the image to restore.

At the CS 2000 Core Manager

- 2 Restore the image from tape. This step requires root privilege.

```
# cd /swd/3pc
# tar xvf /dev/rmt0
```

At the Call Agent Manager

- 3 Log in to the inactive Call Agent and change directory to the location in which to restore the image. Verify that enough disk space exists to hold the image.

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ df -h .
Filesystem                Size      Used Avail Use% Mounted on
172.16.16.24:/nfsserv/3pc/cs/sd00
                           8.0G     6.6G   1.4G   82% /3PC/sd00
```

- 4 Open a file transfer protocol (FTP) session to the CS 2000 Core Manager, and transfer the image. It may be necessary to become the super user to transfer the file.

```
[mtc@hostname image0]$ su
Password:<root_password>
[root@hostname image0]# ftp <core_manager_ip>
Connected to <core_manager_ip>
220 <core_manager_ip> SFTPD Server (Version 19.0.0.0 Nov 14
Name (<core_manager_ip>:mtc): root
Password: <root_passwd>
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd /swd/3pc %% or location of restored image
250 CWD command successful.
ftp> get IMG_TO_RESTORE
local: IMG_TO_RESTORE remote: IMG_TO_RESTORE
227 Entering Passive Mode (10,40,44,6,195,224)
150 Opening data connection for IMG_TO_RESTORE (binary mode)
226 Transfer complete.
225820860 bytes received in 332 secs (6.7e+02 Kbytes/sec)
ftp> bye
221 Goodbye.
```

At the MAP

- 5 Enter the DISKUT level and use the **IMPORT** command to make the image available to the call processing application.

```
CI:
>DISKUT
Disk utility is now active.
DISKUT:
>IMPORT SD00IMAGE0 IMG_TO_RESTORE IMAGE 1020
  IMG_TO_RESTORE : Failed to get record length.
Import: IMG_TO_RESTORE      size: 199 MB
      as: IMG_TO_RESTORE    lrecl: 1020      type: image.

Attempting to import 1 file selected on SD00IMAGE0.

Imported IMG_TO_RESTORE as IMG_TO_RESTORE.

Imported 1 file successfully of 1 attempt on SD00IMAGE0.
>
```

Note: If additional space is needed to import the image, the **IMPORT** command offers to expand the volume.

Copying files from disk to tape

Application

Use this procedure to copy office images or all the files from a disk volume to a digital audio tape (DAT) cartridge.

**CAUTION****Maximum one volume per tape**

Copy no more than one volume onto a tape. To copy multiple volumes, use a separate tape for each volume.

Interval

Perform this procedure when required by your office.

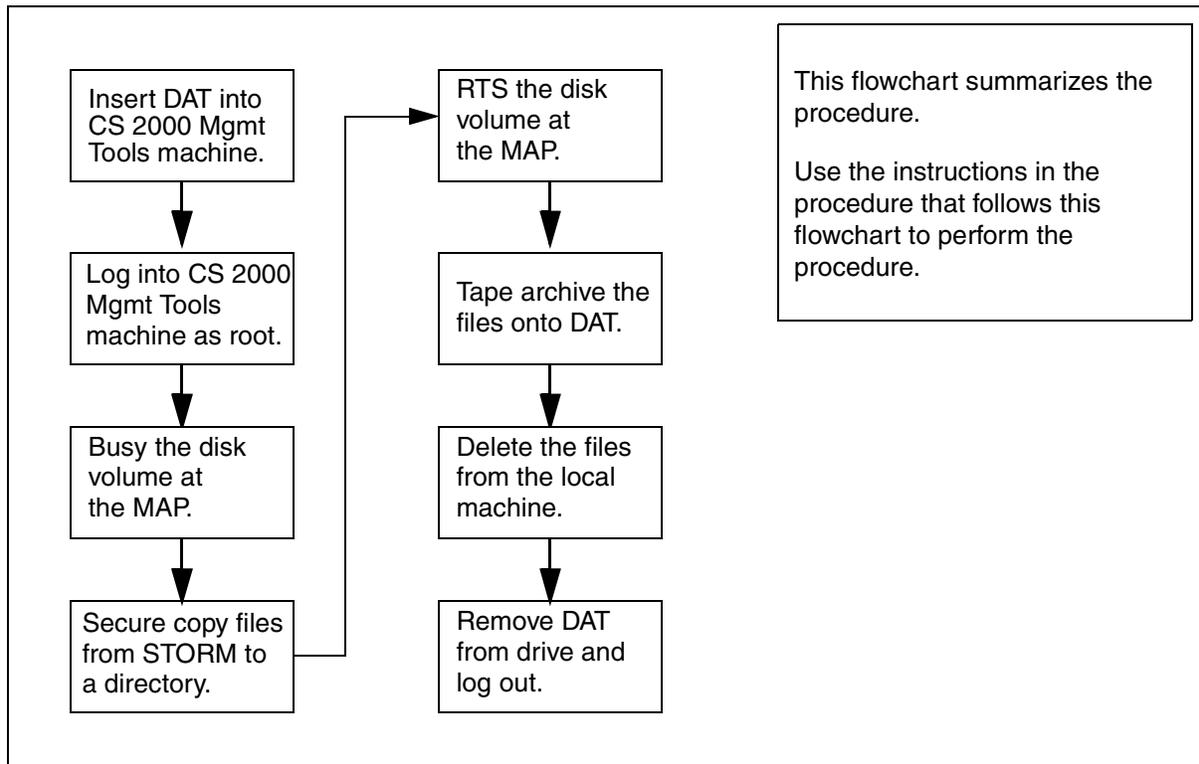
Common procedures

The DAT drive may require periodic cleaning and maintenance. Refer to the product documentation for the CS 2000 Management Tools server hardware.

Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

Summary of copying all files from a disk volume to tape



At the CS 2000 Management Tools server

1



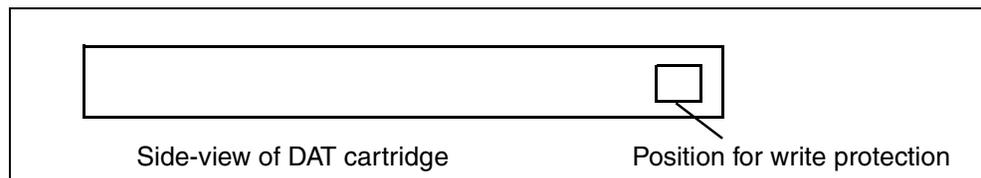
CAUTION

Maximum one volume per tape

Copy no more than one volume onto a tape. To copy multiple volumes, use a separate tape for each volume.

- 2 Determine the volume to backup. Determine the volume from office records or from office personnel. Record the volume name.
- 3 Get a tape cartridge that has the approval of Nortel. All files on the tape will be destroyed. Ensure the tape does not hold valuable data.
- 3 Make sure the tape write protection is at the position that permits recording (closed). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.

Write protection of DAT cartridge



4



WARNING

Static electricity damage

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape. The use of the wrist strap protects against damage caused by electrostatic discharge (ESD).

Insert the DAT tape cartridge into the tape drive.

At a CS 2000 Management Tools server terminal

5 Log in as a maintenance level user. Root permissions are used later in this procedure to write the tape.

6 Change directory to `/data` and create a temporary directory to store the files:

```
$ cd /data
$ mkdir tmp
$ cd tmp
```

7 Determine the environment shell:

```
$ env | grep SHELL
SHELL=/bin/ksh
```

8 Set a filesize creation limit for this instance of the shell:

```
for /bin/ksh:
$ ulimit -f 2929688
for /bin/bash:
$ ulimit -f 1464844
for /bin/csh:
$ limit filesize 1500 megabytes
```

At the MAP

- 9 Enter the DISKADM level and busy the volumes to copy:

```
> DISKADM <sd0x>; BSY <volname>
> QUIT
```

sd0x
is SD00 or SD01

volname
is the name of the volume such as TEMP

The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider [step 11](#) to RTS the volume as soon as possible or convenient after copying the files.

If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.

At a CS 2000 Management Tools server terminal

- 10 Use the secure copy program to copy files from the STORage Management (STORM) unit:

```
$ scp -r "root@<stormip>:</path_to_files>" .
```

stormip
is the IP Address of the STORM unit such as 172.18.96.6

/path_to_files
is the absolute path to the files on the STORM unit to copy such as /nfsserv/3pc/cs/sd00/temp/*

Note: The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "y."

The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.

At the MAP

- 11 Enter the DISKADM level and RTS the copied volumes:

```
> DISKADM <sd0x>; RTS <volname>
> QUIT
```

At a CS 2000 Management Tools server terminal

- 12** Create a file that lists the checksums for all the transferred files:

for /bin/ksh and /bin/bash:

```
$ for i in `ls`  
> do  
> cksum $i >> cksums.txt  
> done
```

for /bin/csh:

```
$ foreach i (`ls`)  
? cksum $i >> cksums.txt  
? end
```

Note: After the first line, press the Return key. The prompt changes until “end” or “done” is entered and the Return key is pressed.

- 13** Become the root user:

```
$ su - root
```

Provide the root password at the prompt.

- 14** Create a tape archive of the current directory:

```
# mt rewind  
# tar cvf /dev/rmt/0 .
```

The tar command prints status to the screen. Wait for the command to complete and the prompt to return.

- 15** To check that files were copied to the tape:

```
# mt rewind  
# tar tvf /dev/rmt/0
```

- 16** Exit from root privilege:

```
# exit  
$
```

The dollar sign command prompt returns.

- 17** Remove the local copies of the files:

```
$ cd ..  
$ rm tmp/*
```

At the CS 2000 Management Tools server**18****WARNING****Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape. The use of the wrist strap protects against damage caused by electrostatic discharge (ESD).

Remove the tape cartridge from the tape drive. Set the tape write protection to the position that does not permit recording (open). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.

Write protection of DAT cartridge

Side-view of DAT cartridge

Position for write protection

- 19** Store the tape cartridge per office procedure.
- 20** This procedure is complete.

Backing up files to DVD-RW

Application

Use this procedure to copy office images or all the files from a disk volume to a digital video disk read write optical disk (DVD-RW).

Note: Rewritable DVDs (DVD+RW) will not work. Use a blank DVD-RW (write once).

**CAUTION****Maximum one volume per DVD-RW**

Copy no more than one volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

Interval

Perform this procedure when required by your office.

Common procedures

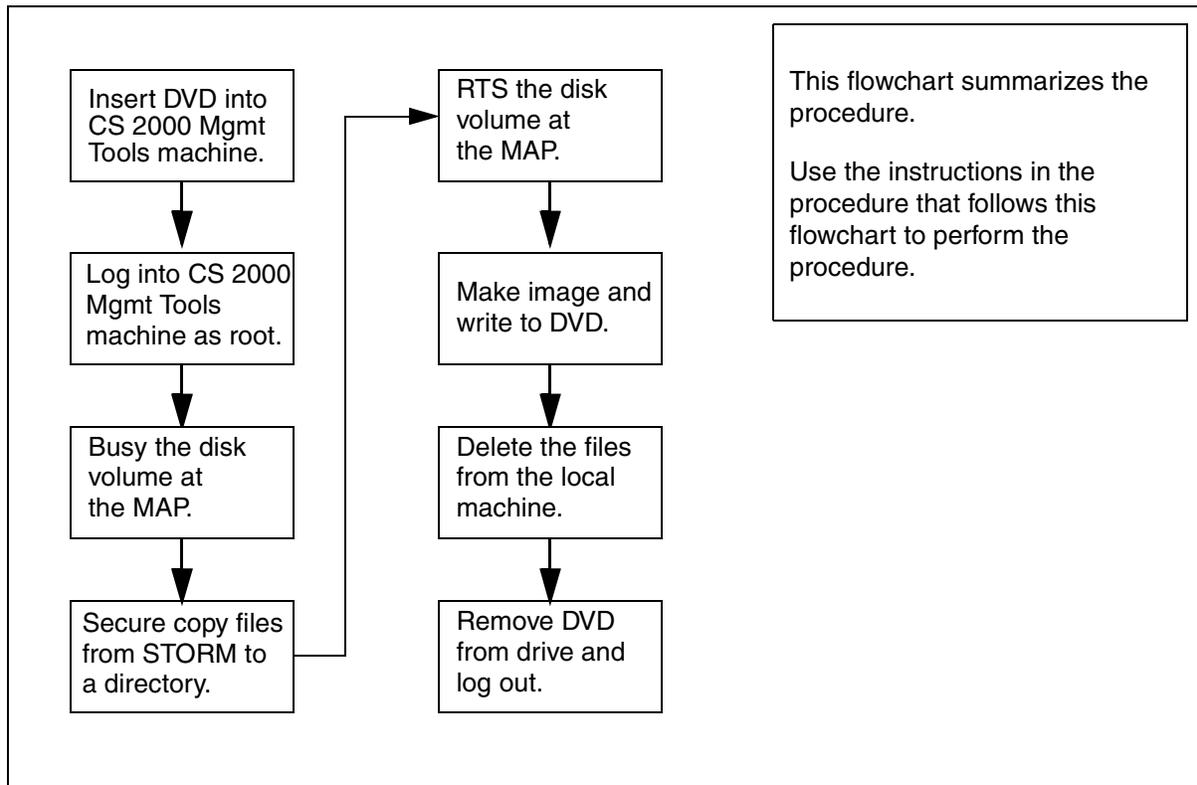
The UNIX commands `mkisofs` and `cdrw` are used. For information about these commands, type **man mkisofs** or **man cdrw** at a terminal prompt.

The IP addresses of the STORM units are determined in [step 1](#). The root password for STORM is needed. The root password for the CS 2000 Management Tools server is needed.

Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

Summary of backing up files to DVD-RW



At the Call Agent Manager

- Quit the maintenance application and then use the mount command to determine the IP addresses of the STORM units.

```
> quit all
[mtc@ip_address mtc]$ mount
```

Determine which STORM unit provides sd00 and which provides sd01. This information is needed in [step 12](#).

```
[mtc@10.40.44.67 mtc]$ mount
/dev/ram0 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0622)
10.40.44.238:/nfsserv/3pc/mtc/tape0 on /TAPE type nfs (rw,rsize=4096...
10.40.44.239:/nfsserv/3pc/mtc/tape1 on /TAPE1 type nfs (rw,rsize=409...
10.40.44.238:/nfsserv/3pc/cs/sd00 on /3PC/sd00 type nfs (rw,rsize=409...
10.40.44.239:/nfsserv/3pc/cs/sd01 on /3PC/sd01 type nfs (rw,rsize=409...
10.40.44.238:/nfsserv/3pc/mtc/log0 on /var/log_mate type nfs (rw,rsi...
10.40.44.239:/nfsserv/3pc/mtc/log1 on /var/log type nfs (rw,rsize=409...
```

At the CS 2000 Management Tools server

2

**CAUTION****Maximum one volume**

Copy only *one* volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

Determine the volume to backup. Determine the volume from office records or from office personnel. Record the volume name.

- 3 Get a DVD-RW that has the approval of Nortel.
- 4 Insert the DVD-RW (write once DVD) into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240 machines, put the DVD-RW into the machine with a lit USER LED on the faceplate.

At a CS 2000 Management Tools server terminal

- 5 Log in as a maintenance level user such as the maint user. Root permissions are used later in this procedure to write the DVD.
- 6 Change directory to `/data` and create a temporary directory to store the files:

```
$ cd /data
```

```
$ mkdir tmp
```

Note: Do not change directory into tmp now. The tmp directory will hold the data to backup.

- 7 Determine the environment shell:

```
$ env | grep SHELL
```

```
SHELL=/bin/ksh
```

- 8 Set a filesize creation limit for this instance of the shell. Choose the **one** that is applicable to your shell. `/bin/ksh` is the default shell:

```
for /bin/ksh:
```

```
$ ulimit -f 2929688
```

```
for /bin/bash:
```

```
$ ulimit -f 1464844
```

```
for /bin/csh:
```

```
$ limit filesize 1500 megabytes
```

At the MAP

9 Determine the approximate size of the image or volume:

| Data to backup | How to determine size | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------|---|-----------|------------------|--------|--------|------|------|--|------------------|-----|---------|------|--------|--|-------------|-----|----|----|------|--|-----|--|------|--------|--|------------------|-----|-------|-----|----|--------|------------------|-------|--------|--------|--------|--------|------------------|-------|--------|------|-------|--------|
| image | <p>Listfile the volume that the image is in:</p> <pre>> DISKUT; LF <vol_name></pre> <pre>> LF SD00ADUMPO</pre> <p>File information for volume SD00ADUMPO: {NOTE: 1 BLOCK = 512 BYTES }</p> <pre>-----</pre> <table border="1"> <thead> <tr> <th>FILE NAME</th> <th>O R I O O V FILE</th> <th>MAX</th> <th>NUM OF</th> <th>FILE</th> <th>LAST</th> </tr> <tr> <th></th> <th>R E T P L L CODE</th> <th>REC</th> <th>RECORDS</th> <th>SIZE</th> <th>MODIFY</th> </tr> <tr> <th></th> <th>G C O E D D</th> <th>LEN</th> <th>IN</th> <th>IN</th> <th>DATE</th> </tr> <tr> <th></th> <th>C N</th> <th></th> <th>FILE</th> <th>BLOCKS</th> <th></th> </tr> </thead> <tbody> <tr> <td>S040210135002HIS</td> <td>O V</td> <td>0 255</td> <td>276</td> <td>27</td> <td>040210</td> </tr> <tr> <td>S040210135002_CM</td> <td>I F Y</td> <td>0 1020</td> <td>220288</td> <td>438855</td> <td>040210</td> </tr> <tr> <td>S040210135002_MS</td> <td>I F Y</td> <td>0 1020</td> <td>7803</td> <td>15546</td> <td>040210</td> </tr> </tbody> </table> <pre>-----</pre> <p>The approximate size of the image in megabytes is NUM OF RECORDS IN FILE / 1000: 220288 / 1000 = 220 MB</p> | FILE NAME | O R I O O V FILE | MAX | NUM OF | FILE | LAST | | R E T P L L CODE | REC | RECORDS | SIZE | MODIFY | | G C O E D D | LEN | IN | IN | DATE | | C N | | FILE | BLOCKS | | S040210135002HIS | O V | 0 255 | 276 | 27 | 040210 | S040210135002_CM | I F Y | 0 1020 | 220288 | 438855 | 040210 | S040210135002_MS | I F Y | 0 1020 | 7803 | 15546 | 040210 |
| FILE NAME | O R I O O V FILE | MAX | NUM OF | FILE | LAST | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | R E T P L L CODE | REC | RECORDS | SIZE | MODIFY | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | G C O E D D | LEN | IN | IN | DATE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | C N | | FILE | BLOCKS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| S040210135002HIS | O V | 0 255 | 276 | 27 | 040210 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| S040210135002_CM | I F Y | 0 1020 | 220288 | 438855 | 040210 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| S040210135002_MS | I F Y | 0 1020 | 7803 | 15546 | 040210 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| volume | <p>Listvols the volume with the megabyte option:</p> <pre>> DISKUT; LV SD00TEMP MB</pre> <p>Subtract FREE MBYTES from TOTAL MBYTES to determine the approximate size of the volume: 400 - 340 = 60 MB</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

10 If backing up an entire volume, enter the DISKADM level and busy the volume:

```
> QUIT ALL
> DISKADM <sd0x>; BSY <volname>
> QUIT
sd0x
is SD00 or SD01
```

volname

is the name of the volume such as TEMP or ADUMP0

The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider [step 13](#) to RTS the volume as soon as possible or convenient after copying the files.

If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.

At a CS 2000 Management Tools server terminal

- 11 Ensure that enough disk space is available for the data to record. Twice the space determined in [step 9](#) is needed:

```
$ df -k /data
```

The free space on the device that /data is mounted is printed. The value for “avail” is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes. Ensure that there is free space for two times the size of the data to record.

```
$ df -k /data
```

| Filesystem | kbytes | used | avail | capacity | Mounted on |
|-----------------|---------|--------|---------|----------|------------|
| /dev/md/dsk/d20 | 3082223 | 144125 | 2876454 | 5% | /data |

```
2876454 / 1000 = 2876 MB free
```

- 12 Secure copy the files from the STORM unit to the /data/tmp directory created in [step 6](#). Enter the root password for the STORM unit when prompted:

```
$ scp -r "root@<stormip>:</path_to_files>" /data/tmp
```

Note: There is a space before the /data/tmp argument.

stormip

is the IP Address of the STORM unit such as 10.40.44.238. Use the value determined in [step 1](#).

/path_to_file

is the absolute path to the files on the STORM unit to copy such as /nfsserv/3pc/cs/sd00/temp/*

Example

Copy an office image named S040210135002_CM from SD00ADUMP0:

```
$ scp -r
"root@<stormip>:/nfsserv/3pc/cs/sd00/adump0/S04021
0135002_CM" /data/tmp
```

Note: The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "yes." The root password for the STORM unit is needed.

The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.

At the MAP

- 13 If the volume was busied in [step 10](#), enter the DISKADM level and RTS the copied volumes:

```
> DISKADM <sd0x>; RTS <volname>
> QUIT
```

At a CS 2000 Management Tools server terminal

- 14 If only image files are transferred, and the files do not end in _CM or _MS, rename the files to include the file attributes IMG and 1020:

```
$ mv <image_filename> <image_filename>.IMG1020
```

Example

```
$ mv raleigh_04wk06 raleigh_04wk06.IMG1020
```

Note: If the name of the image already ends in _CM or _MS, skip this step.

- 15 Change directory out of /data/tmp and make an ISO9660 image named dvdimage.iso with Rock Ridge extensions from the files in tmp:

```
$ cd /data
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
```

Status is printed to the terminal:

Create dvdimage.iso with mkisofs command

```
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
4.56% done, estimate finish Tue Feb 10 14:52:00 2004
9.11% done, estimate finish Tue Feb 10 14:52:00 2004
13.67% done, estimate finish Tue Feb 10 14:52:00 2004
...
95.67% done, estimate finish Tue Feb 10 14:52:05 2004
Total extents actually written = 109764
Total translation table size: 0
Total rockridge attributes bytes: 421
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 8000
109764 extents written (214 Mb)
$
```

- 16 Become the root user:

```
$ su - root
```

Provide the root password at the prompt.

- 17 Optionally verify the ISO9660 image:

```
# lofiadm -a /data/dvdimage.iso /dev/lofi/1
# mount -F hsfs /dev/lofi/1 /mnt
# ls -as1 /mnt
```

The contents of the ISO 9660 image are displayed. These files will be written to the DVD-RW. Ensure the display looks similar to the following image.

Note 1: *If the lofiadm command reports the error “lofiadm: could not map file /data/dvdimage.iso to /dev/lofi/1: Device busy,” then the first loopback file driver is already in use. Reenter the command and substitute /dev/lofi/2 for /dev/lofi/1. Continue incrementing the number until the command succeeds and then use the successful value in the mount command.*

Note 2: *If the mount command reports the error “mount: /dev/lofi/1 is already mounted, /mnt is busy, or allowable number of mount points exceeded,” unmount the /mnt directory with the **umount /mnt** command and reenter the mount command.*

List contents of the ISO 9660 image

```
# lofiadm -a /data/dvdimage.iso /dev/lofi/1
# mount -F hsfs /dev/lofi/1 /mnt
# ls -asl /mnt
total 431996
  4 dr-xr-xr-x  2 root  sys      2048 Apr 20 09:48 .
  2 drwxr-xr-x 33 root  root    1024 Apr 20 11:16 ..
431990 -rw-r--r--  1 maint maint 221178840 Apr 20 09:47 IMG_TO_BACKUP.img1
```

- 18 Determine the name of the DVD-RW device:

```
# cdrw -l
```

All optical disk devices are printed.

Determine the DVD-RW device name

```
# cdrw -l
Looking for CD devices...
  Node                Connected Device                Device type
-----+-----+-----
  cdrom0              | TOSHIBA DVD-ROM SD-R6012 1033 | CD Reader/Writer
```

Note: *If the command responds with “No CD writers found or no media in the drive,” and the CS 2000 Management Tools server is a cluster then verify that the DVD-RW is placed in the active unit. The active unit is identified by a lit USER LED on the face of the unit.*

- 19 Optionally simulate (-S flag) recording the image to verify that the ISO 9660 image can be recorded on the DVD-RW. This step requires approximately 10 minutes:

```
# cdrw -d <dvd_dev> -S -i /data/dvdimage.iso
```

Example

```
# cdrw -d cdrom0 -S -i /data/dvdimage.iso
```

*The CDROM tray ejects after this simulation. **Close the CDROM tray and continue this procedure to write the DVD-RW.***

- 20 Record the image. This step requires approximately 10 minutes:

```
# cdrw -d <dvd_dev> -i /data/dvdimage.iso
```

Example

```
# cdrw -d cdrom0 -i /data/dvdimage.iso
```

If the error response "Media in the device is not writable" is returned, verify that the CDROM tray is closed.

Approximately two minutes pass before progress is printed to the screen. After the first 1% is written, each additional percent requires about two seconds.

CDRW command progress

```
# cdwr -d cdrom0 -i /data/dvdimage.iso
Initializing device...done.
Preparing to write DVD
Writing track 1 ... 99 %
```

Approximately nine minutes pass before the command completes.

```
done.
done.
Finalizing (Can take up to 4 minutes)...done.
$
```

*The CDROM tray on the CS 2000 Management Tools server ejects. **Close the CDROM tray and continue this procedure to verify the contents of the DVD-RW.***

- 21** Check that ISO9660 image recorded correctly:

```
# ls -asl /cdrom/cdrom
```

The contents of the DVD-ROM are printed.

- 22** Unmount the DVD-RW, eject it, and exit from root privilege:

```
# eject cdrom
```

If the ISO 9660 image was verified with the lofiadm command, remove the loopback file driver device:

```
# umount /mnt
```

```
# lofiadm -d /dev/lofi/1
```

Note: If /dev/lofi/2 was used above, substitute /dev/lofi/2 in this command.

Exit from root privilege:

```
# exit
```

```
$
```

The dollar sign command prompt returns.

- 23** Remove the local copies of the files:

```
$ rm /data/tmp/*  
$ rm /data/dvdimage.iso
```

At the CS 2000 Management Tools server

- 24** Remove the DVD-RW from the tray and close the tray. Label the DVD-RW.
- 25** Store the DVD-RW per office procedure.
- 26** This procedure is complete.

Restoring files from a DVD-RW

Application

Use this procedure to restore office images from a digital video disk read write optical disk (DVD-RW). Do not restore an image and overwrite one with the same name.

To restore a volume from DVD-RW, contact Nortel support personnel.

Interval

Perform this procedure when required by your office.

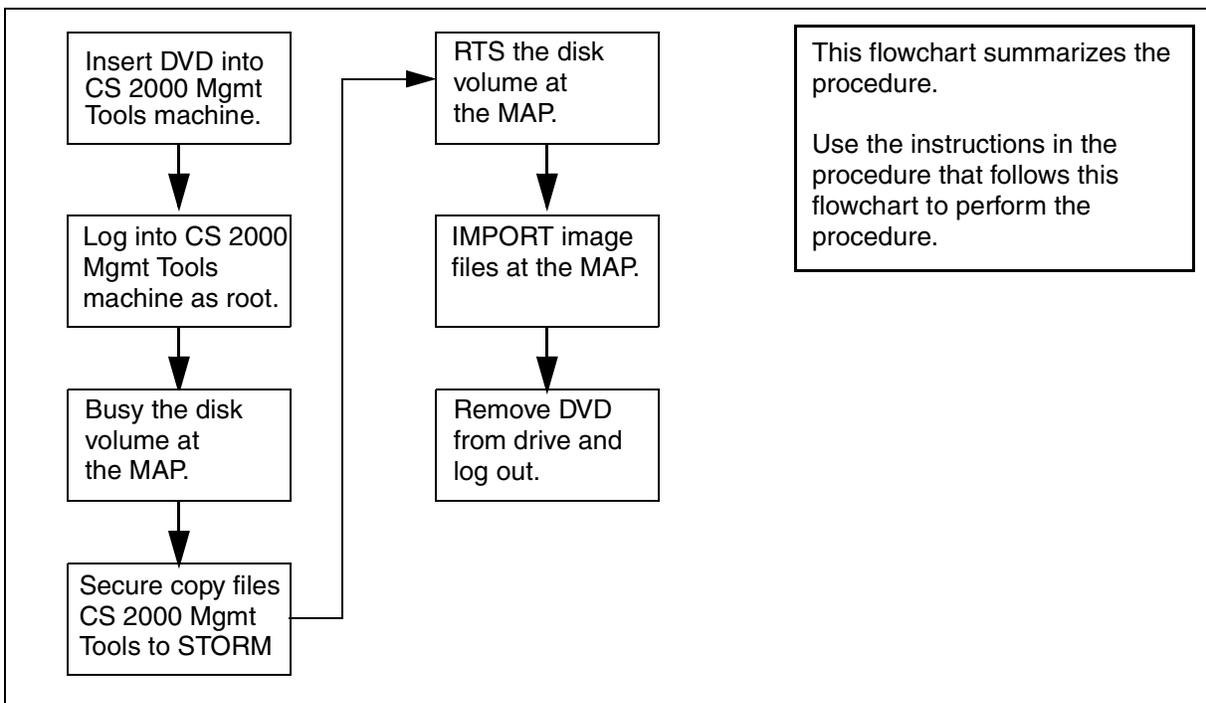
Common procedures

Understanding of the **IMPORT** command in DISKUT, **SCANF** for listing volumes, and the **CBF**, **LBF**, and **SBF** commands in ITOCCI is required. The IP addresses of the STORM units are needed. Use the **mount** command from a Call Agent card to determine the addresses.

Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

Summary of restoring files from a DVD-RW



At the CS 2000 Management Tools server

- 1 Insert the DVD-RW into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240s, put the DVD in the unit with the USER LED lit.
Volume management software on the CS 2000 Management Tools server operating system mounts the DVD-RW.
- 2 List the contents:

```
$ ls -as /cdrom/cdrom0
```

The contents of the DVD are printed.
- 3 Change directory to the DVD-RW:

```
$ cd /cdrom/cdrom0
```

At the MAP

- 4 Enter the DISKADM level and busy the volumes to copy:

```
> DISKADM <sd0x>; BSY <volname>
```

```
> QUIT
```

sd0x

is SD00 or SD01

volname

is the name of the volume such as TEMP

The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider [step 6](#) to RTS the volume as soon as possible or convenient after copying the files.

If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.

At a CS 2000 Management Tools server terminal

- 5 Secure copy the files from the DVD-RW on the CS 2000 Management Tools server to one STORage Management (STORM) unit:

```
$ scp "<image_files>"  
"root@<stormip>:</path_to_files>"
```

image_files

is the file name for a single image file, or a wildcard expression such as "*_CM"

stormip

is the IP Address of the STORM unit such as 172.18.96.6

/path_to_files

is the absolute path to the files on the STORM unit to place the files such as /nfsserv/3pc/cs/sd00/image1

Example

Copy an office image named S040210135002_CM to SD00IMAGE1:

```
$ scp S040210135002_CM  
"root@<stormip>:/nfsserv/3pc/cs/sd00/image1"
```

Note: The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "y."

The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.

At the MAP

6 Enter the DISKADM level and RTS the volume:

```
> DISKADM <sd0x>; RTS <volname>  
> QUIT
```

7 Enter the DISKUT level and IMPORT the image files:

```
> DISKUT; IMPORT SD00IMAGE1  
> QUIT
```

The status of the IMPORT command is printed.

IMPORT result

```
> IMPORT SD00IMAGE1  
Attempting to import 1 fileselected on SD00IMAGE1.  
Imported S040210135002_CM as S040210135002_CM IMAGE 1020.  
Imported 1 file successfully of 1 attempt on SD00IMAGE1.
```

8 List the contents of the volume so the file can be added to the Image Table of Contents (ITOC) in the next step:

```
> SCANF SD00IMAGE1
```

The contents of the volume are printed.

- 9 Enter ITOCCI and register the image in the ITOC:
- ```
> ITOCCI
> SBF CM S040210135002_CM <itoc_pos> <alr_flag>
```
- itoc\_pos**  
is an integer between 0 and 15, and is a free position in the ITOC.
- alr\_flag**  
if this image should be booted for the next restart, specify **ALR**. Otherwise, leave the field blank.
- Note:** To determine if a free position is available, use the **LBF CM** command. If all positions are used, clear the file in position 15. Determine which volume the position 15 is on, use **SCANF** to list that volume, and then use the **CBF CM FILE <image\_name>** command.

***At a CS 2000 Management Tools server terminal***

- 10 Unmount the DVD-RW, eject it, and exit from root privilege:
- ```
$ eject cdrom
```

At the CS 2000 Management Tools server

- 11 Remove the DVD-RW from the tray and close the tray.
- 12 Store the DVD-RW per office procedure.
- 13 This procedure is complete.

Scheduling automatic image taking

Application

Use this procedure to enable and schedule automatic image taking. This procedure makes a record of the office image to a disk volume.

Interval

This procedure is a task performed on the decision of the office manager.

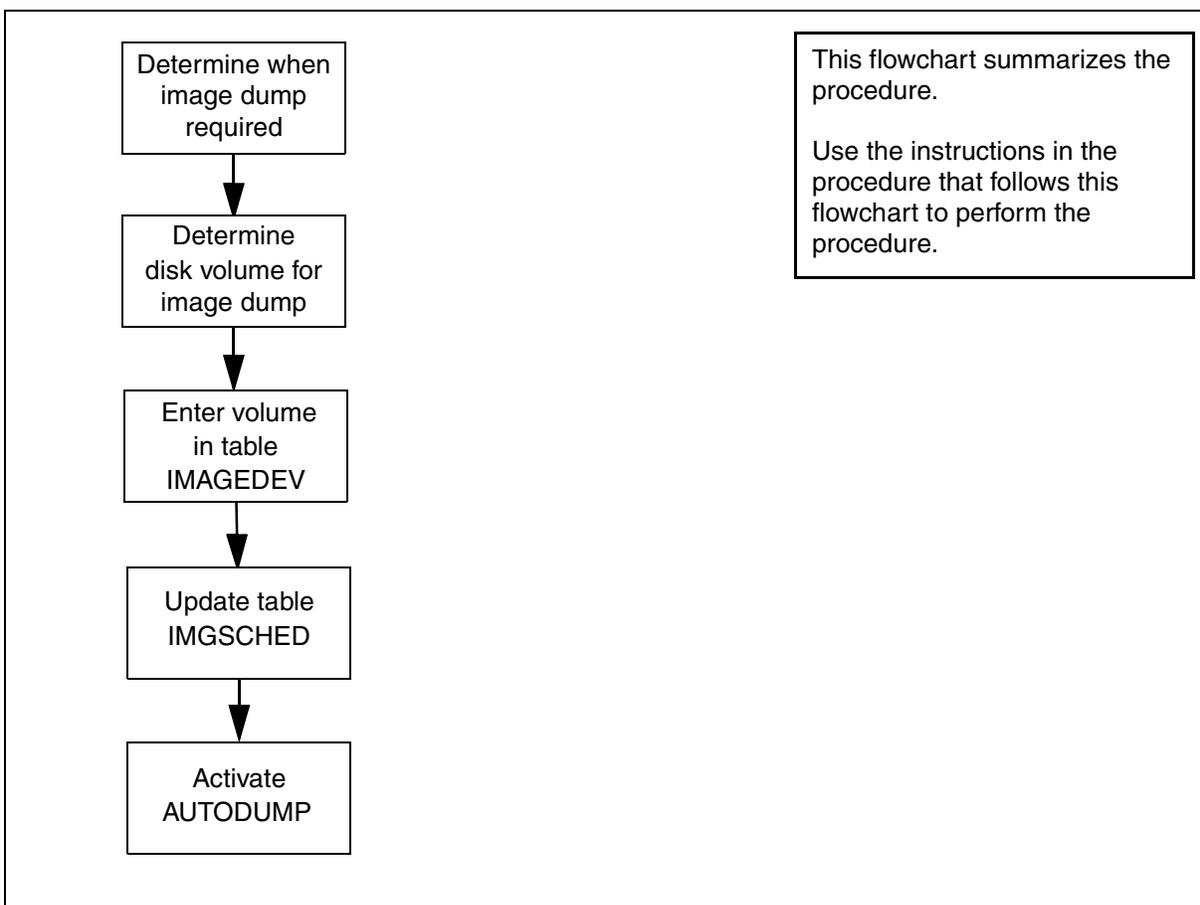
Common procedures

There are no common procedures.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Summary of scheduling automatic image taking



At your current location

- 1 Determine and record the days and times to have an office image dump. Determine the days and times from office personnel or office records.
- 2 Determine and record the volume names that store the image files. Determine the volume names from office personnel or office records.

At the MAP

- 3 Access the CI level of the MAP:

```
>QUIT ALL
```

- 4 Access the disk utility level:

```
>DISKUT
```

Example of a MAP response:

```
Disk utility is now active.
DISKUT:
```

- 5 List the volumes:

```
>LISTVOLS
```

Example of a MAP response:

```
>LV
Volumes found:
-----
NAME                TYPE      TOTAL    FREE TOTAL  OPEN  ITOC   LARGEST
                   BLOCKS   BLOCKS  FILES  FILES  FILES  FREE
SEGMENT
-----
SD00IMAGE           STD      1638400  1063334    2     0     1    1063334
SD00IMAGE1          STD      1638400   771242    3     0     4     771242
SD00PERM             STD       409600   409100    8     0     0     409100
SD00TEMP            STD       409600   406595   93     0     0     406595
SD00SBA              STD      2097152     0    323     0     0         0
SD00AMA0            STD       122880   122880    0     0     0     122880
SD00AMA1            STD       122880   122880    0     0     0     122880
...
SD01DLG2            STD       122880   122880    0     0     0     122880
SD01DLG3            STD       122880   122880    0     0     0     122880
SD01JF              STD       122880   122880    0     0     0     122880
SD01SCRATCH         STD       204800   189313   13     0     0     189313
SD01PAT             STD       204800   203250  297     0     0     203250
Total number of volumes listed: 30.
>
```

6 Determine which volume in step 5 has the volume name that stores the image files.

7 Quit the MAP disk utility level:

>QUIT

8 Access table IMAGEDEV:

>TABLE IMAGEDEV

9 List the tuples in table IMAGEDEV:

>LIST ALL

Example of a MAP response:

```
TOP
          VOLNAME          ACTIVE
-----
          SD00IMAGE1          Y
BOTTOM
```

Example of a MAP response to an empty table IMAGEDEV:

EMPTY TABLE

10 Check if the image volume from office records is in the list of table IMAGEDEV in step 9.

| If the image volume is | Do |
|------------------------|-------------------------|
| in table IMAGEDEV | step 15 |
| not in table IMAGEDEV | step 11 |

11 To add a tuple for the image volume recorded in step 2, type.

>ADD volume_name Y

volume_name

is the name of the volume used for automatic image dumps

Y

is confirmation that the volume is active

Example

Add SD00IMAGE1 as the active volume for image dumping.

>ADD SD00IMAGE1 Y

12 Confirm the command:

>Y

Example of a MAP response:

TUPLE ADDED

- 13** Check the tuple addition to table IMAGEDEV:

>LIST ALL

The tuples in the table are listed. Ensure that the new tuple is listed.

- 14** Quit from table IMAGEDEV:

>QUIT

- 15** Access table IMGSCHEM:

>TABLE IMGSCHEM

- 16** List all the tuples:

>LIST ALL

Example of a MAP display:

```
>LIST ALL
TOP
      DAY      DUMPHOUR  DUMPMIN  CMMS      ISN      USESDM  ACTIVE
-----
      MONDAY      21         0        N         N         N         N
      TUESDAY      21         0        N         N         N         N
      WEDNESDAY    21         0        N         N         N         N
      THURSDAY     21         0        N         N         N         N
      FRIDAY       21         0        N         N         N         N
      SATURDAY     21         0        N         N         N         N
      SUNDAY       21         0        N         N         N         N
BOTTOM
>
```

Note 1: Fields DUMPHOUR and DUMPMIN control the time at which the dump performs. The default time is 21:00. Modify the time according to separate office requirements. Perform image dumps during hours that have minimum traffic.

Note 2: Field ACTIVE cannot be set to Y if both the CMMS and ISN fields are N.

- 17** Access the tuple for the first day to activate an automatic image dump:

>POSITION <day>

- day**
is the day for which to activate automatic image taking, for example, MONDAY
- 18** Edit the tuple:
>**CHANGE**
- 19** Confirm the command:
>**Y**
Example of a MAP response:
DUMPHOUR: 21
- 20** Enter the required dump hour:
>**dump_hour**
dump_hour
is the dump hour you must enter, for example, 21
Example of a MAP response:
DUMPMIN: 0
- 21** Enter the required dump minutes:
>**dump_minutes**
dump_minutes
is the dump minutes, for example, 30
Example of a MAP response:
CMMS: N
- 22** Enable the automatic image dump on nodes CM and MS, if an MS is available:
>**Y**
Example of a MAP response:
ISN: N
- 23** Do not enable the Intelligent Switch Network image dump:
>**N**
Example of a MAP response:
USESDM: N
- 24** Do not enable the USESDM option:
>**N**

Example of a MAP response:

ACTIVE: N

- 25** Make the automatic image dump active for the selected day:

>Y

Example of a MAP response:

TUPLE TO BE CHANGED:

 MONDAY 21 30 Y N Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

- 26** Confirm the tuple change:

>Y

Example of a MAP response:

TUPLE CHANGED

- 27** Check the tuple revisions to table IMGSCHEd:

>LIST ALL

| If all the tuple entries are | Do |
|------------------------------|---|
| complete | step 28 |
| not complete | Repeat steps 17 to 26 for each day an automatic image dump is needed. |

- 28** Quit from table IMGSCHEd:

>QUIT

- 29** Activate the autodump facility for the days and times in table IMGSCHEd:

>AUTODUMP ON

Example of a MAP response:

SCHEDULED-Image Dump is ON.

Next scheduled dump is MONDAY at 21:30 hours.
Next image to be dumped on SD00IMAGE1.

Note: The MAP response identifies the disk and volume name that the image dumps to. The switch software selects from table IMAGEDEV the disk and volume to dump the image to.

- 30** To check the status of automatic image taking:

>AUTODUMP STATUS

Example of a MAP response

Successful Image: 030826_CM
 Taken: 2003/08/26 21:47:32:04.138 TUE.
 On Volume: SD00IMAGE1

SCHEDULED-Image Dump is ON.

RETAIN option is ON.

Next scheduled dump is MONDAY at 21:30 hours.
 Next image to be dumped on SD00IMAGE1.

- 31** Check that automatic image taking is on. In the example of a MAP response of step [30](#), the text SCHEDULED-Image Dump is ON indicates the automatic image taking is on.

| If SCHEDULED-Image Dump is | Do |
|----------------------------|-------------------------|
| ON | step 32 |
| OFF | step 36 |

- 32** Check that the RETAIN option is off. In the example of a MAP response of step [30](#), the text RETAIN option is ON indicates the retain option is on.

| If RETAIN option is | Do |
|---------------------|-------------------------|
| ON | step 33 |
| OFF | step 36 |

Note: Setting RETAIN to off is usually preferred. The RETAIN option determines if the boot pointer is set to the newly dumped image (RETAIN is OFF), or if it remains set to its current setting (RETAIN is ON).

- 33** Change the RETAIN option to OFF:

>AUTODUMP RETAIN

Example of a MAP response:

RETAIN option is currently ENABLED.
 This option RETAINS the PRIMARY LOAD ROUTE.
 The PRIMARY LOAD ROUTE should be initially set per NTP.

The RETAIN option will be DISABLED.
Please confirm ("YES", "Y", "NO", or "N"):

34 Confirm the command:

>YES

Example of a MAP response:

RETAIN option DISABLED.

35 Check the status of automatic image taking, type:

>AUTODUMP STATUS

and press the enter key.

Example of a MAP response

Successful Image: 030826_CM
Taken: 2003/08/26 21:47:32:04.138 TUE.
On Volume: SD00IMAGE1

SCHEDULED-Image Dump is ON.

RETAIN option is OFF.

Next scheduled dump is MONDAY at 22:30 hours.
Next image to be dumped on SD00IMAGE1.

36 If the RETAIN option cannot be set to OFF, or table provisioning fails, call the next level of support.

37 You have completed this procedure.

How to change REx Tst (routine exercise test) intensity

Application

REx Tst intensity cannot be configured on a Call Agent. Below are listed the two types of REx Tsts that run on a Call Agent. Every night, a BASE class REx Tst is run, and on Thursday night, a FULL class REx Tst is run.

If the CS 2000 - Compact is configured with Message Controller cards, then a BASE class REx Tst is run on the one Message Controller on the Thursday night after the Call Agent completes a FULL class REx Tst. One Message Controller runs the test, and the next week, the other Message Controller runs the test.

The classes of REx tests have the following differences:

- BASE class of REx Tst is:
 - Synchronization is dropped.
 - An in service image test of the inactive call processing application, on the inactive Call Agent card.
 - Synchronization is restored.
 - BASE REx Tsts run each day of the week except Thursday.
- FULL class of REx Tst is:
 - Synchronization is dropped.
 - The inactive Call Agent is shutdown, reset, the Shelf Controller initiates hardware diagnostics on the card, and then the card boots the 3plinuximage platform software load.
 - An image test is run.
 - Synchronization is restored.
 - FULL REx tests run Thursday nights.

Common procedures

There are no common procedures.

Action

REx Tst intensity cannot be configured. However, to enable REx Tsts, tuple NODEREXCONTROL in table OFCVAR must be set to 'Y.' Refer to *DMS-100 Office Parameter Reference Manual*, 297-8001-855 (NA) or 297-9051-855 (EMEA) for information about NODEREXCONTROL.

CS 2000 SAM21 Manager procedures

The CS 2000 SAM21 Manager manages the hardware and hardware states of the Call Agent and all the cards in the SAM21 shelf.

Card icons

Use this procedure to determine the state of a card through the CS 2000 SAM21 Manager client.

At the CS 2000 SAM21 Manager client

- 1 Review the following figure and determine the card icons that apply.

The screenshot shows a rack of 17 slots. Slots 7, 9, 12, and 13 are highlighted in red. Slot 7 has a '2C' callout and 'SC / ATM (Not Provisioned)'. Slot 9 has a '1C' callout and 'SC / ATM (Not Provisioned)'. Slot 12 has a '1M' callout and 'GWC-5-LUNIT-0'. Slot 13 has a '1C' callout and 'No Service'. Other slots contain various icons and labels like 'GWC-0-LUNIT-0', 'No Service', 'GWC-2-LUNIT-0', 'GWC-3-LUNIT-0', 'Call Agent', 'GWC-4-LUNIT-0', and 'Sled 1'.

| Slot | Label | Icon | Callout |
|------|----------------------------|---------|---------|
| 1 | GWC-0-LUNIT-0 | Icon 1 | |
| 2 | GWC-1-LUNIT-0 | Icon 2 | |
| 3 | No Service | Icon 3 | |
| 4 | GWC-2-LUNIT-0 | Icon 4 | |
| 5 | GWC-3-LUNIT-0 | Icon 5 | |
| 6 | Call Agent | Icon 6 | |
| 7 | SC / ATM (Not Provisioned) | Icon 7 | 2C |
| 8 | | | |
| 9 | SC / ATM (Not Provisioned) | Icon 9 | 1C |
| 10 | | | |
| 11 | GWC-4-LUNIT-0 | Icon 11 | |
| 12 | GWC-5-LUNIT-0 | Icon 12 | 1M |
| 13 | No Service | Icon 13 | 1C |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |

Legend:

1. locked-disabled-offduty
2. locked-disabled-offline (reinserted card)
3. locked-disabled-offline (new card)
4. locked-disabled-in test
5. locked-disabled-failed
6. unlocked-disabled-offduty
7. unlocked-enabled-none (with alarms)
9. locked-disabled-none or locked-disabled-degraded (with alarms)
11. unlocked-enabled-degraded
12. locked-disabled-none (with alarms)
13. locked-disabled-failed (no application and with alarms)

Note: These states also apply to SAM21 Shelf Controllers.

- 2 To view the card state tab, right-click on the card icon and select Card View from the card context menu. In the Card View window that opens, select the States tab.
- 3 Determine the next action.

| State | Possible action |
|---|--|
| locked-disabled-offduty   | Wait for the firmware flash to complete. Verify that the card changes to the locked-disabled-none state. If the card transitions to locked-disabled-degraded, follow the suggestions for that state. |
| unlocked-disabled-offduty  | For Call Agent cards, this state also represents the restart and reload of the call processing application during a routine exercise test (REXTst). When the SAM21 Shelf Controller performs its boot audit, any card that is not running or booting is set to this state until the SAM21 Shelf Controller recovers the card. |
| locked-disabled-offline (new card)  | Right-click on the card icon and select Assign Service from the card context menu. Select the correct service from the Assign Service window. If the question mark icon does not disappear, open the Card View and view the States tab. If the history text area indicates that service assignment failed because the service type is incompatible with the hardware, either replace the card with the correct hardware type, or unassign service from the shelf view and then assign the correct service type. |

| State | Possible action |
|---|---|
| locked-disabled-offline (reinsertion)   | <p>Wait for SAM21 Shelf Controller to recognize the card and reinstate the provisioning information. The question mark icon disappears and the card transitions to a new state. Refer to the suggestions for the new state.</p> <p>If the question mark icon does not disappear, open the Card View window and view the States tab. If the history text area indicates that service assignment failed because the service type is incompatible with the hardware, either replace the card with the correct hardware type, or unassign service from the shelf view and then assign the correct service type.</p> <p>If the history text area indicates that the service assignment failed because the IP address is already reserved by another unit, contact network engineering to determine if another unit is misconfigured, or if this unit should be reconfigured.</p> |
| locked-disabled-none or locked-disabled-degraded   | <p>Unlock the card by right-clicking on the card icon and select Unlock from the card context menu.</p> <p>Rerun diagnostics if the CS 2000 SAM21 Manager client generates a Degraded state Unlock confirmation window. If diagnostics fail a second time, replace the card and contact Nortel support personnel.</p> <p>Note: The active SAM21 Shelf Controller generates 2 critical alarms when the inactive SAM21 Shelf Controller is locked. A locked-disabled- degraded state for non system slot (NSS) cards is also alarmed.</p> |
| locked-disabled-failed   | <p>This card is inaccessible. Verify the following items:</p> <ul style="list-style-type: none"> • SAM21 Shelf Controllers are in service • If the SAM21 Shelf Controllers are in service, reinsert the card. If the card is not recognized, replace the card. If the replacement card does not enter unlocked-enabled-none, contact Nortel support personnel. |
| locked-disabled-in test   | <p>Wait for diagnostics to complete. Verify that the card changes to the locked-disabled-none state. Optionally monitor diagnostics progress from the Card View window.</p> |

| State | Possible action |
|---|---|
| unlocked-enabled-degraded  | <p>This card failed one or more diagnostics and was Unlocked. See Additional information below.</p> <p>This card may not be providing service or may be unreliable. Lock and run diagnostics on this card. If the card fails diagnostics, replace this card and contact Nortel support personnel.</p> |
| locked-disabled-none and alarmed  | <p>This card has taken more than three minutes to complete a lock or unlock request. The alarm clears when the card completes the request or is removed from the shelf.</p> |
| locked-disabled-failed (no application)   | <p>The active SAM21 Shelf Controller detects a card in the slot, but cannot through the backplane to the card. Reinsert the card.</p> |

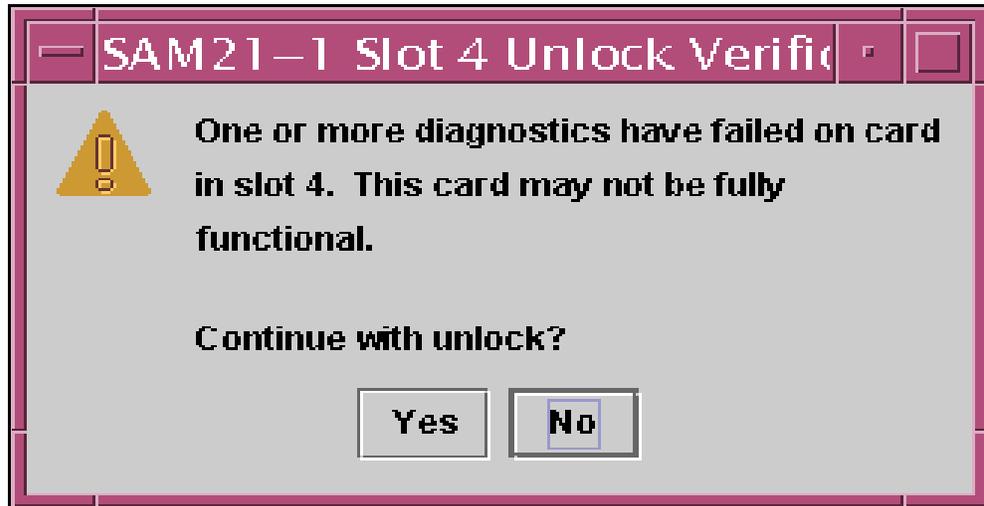
Note: Refer to the Fault Management document for the affected card type.

- 4 This procedure is complete.

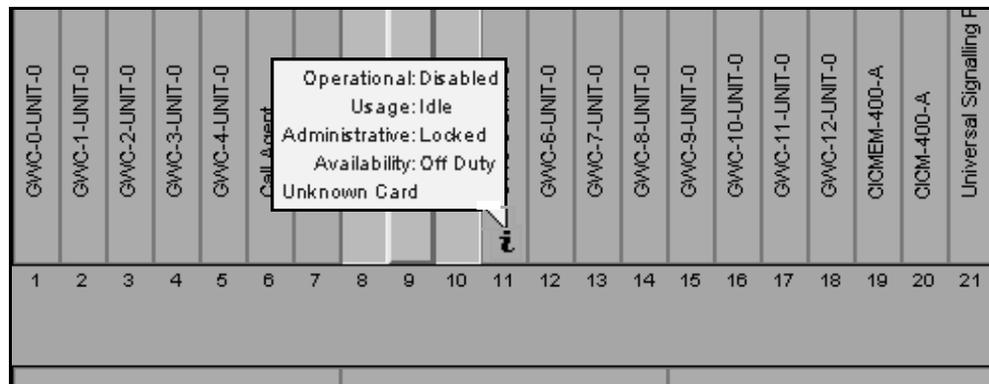
Additional information

The CS 2000 SAM21 Manager application opens the following window if a card failed a diagnostic test and an unlock request is made. Run brief and full diagnostics. If the card fails a second time, replace the card and contact Nortel support personnel.

Degraded state Unlock confirmation window



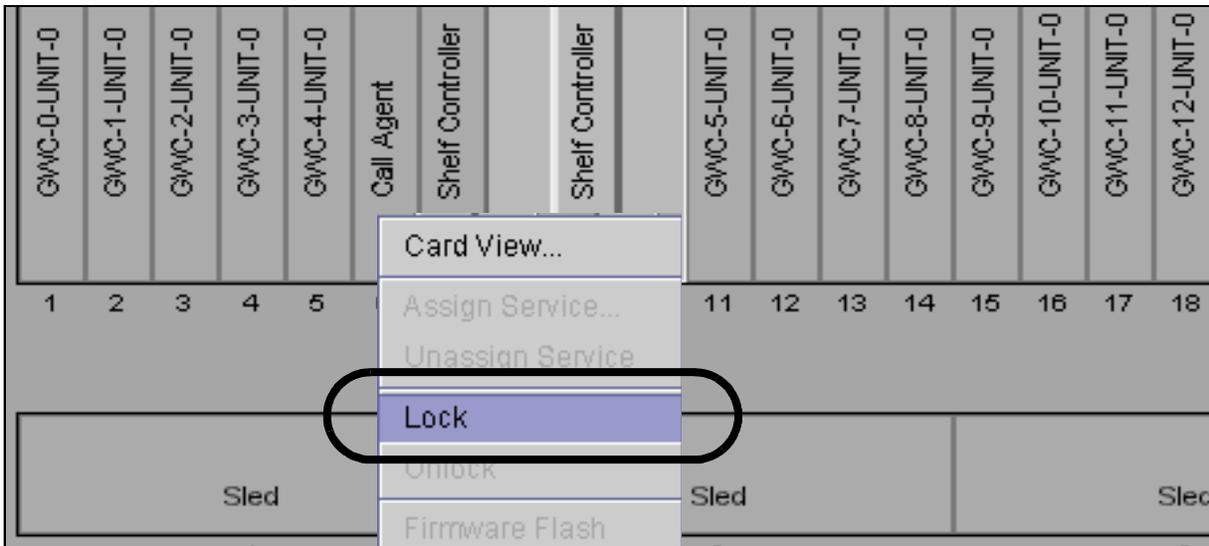
An additional shelf view card icon indicates that the CS 2000 SAM21 Manager client cannot display all the card icons. Click this information icon to view the card state information in a balloon. This icon normally indicates that the card type is not supported for the current release of the CS 2000 SAM21 Manager software.



Running diagnostics

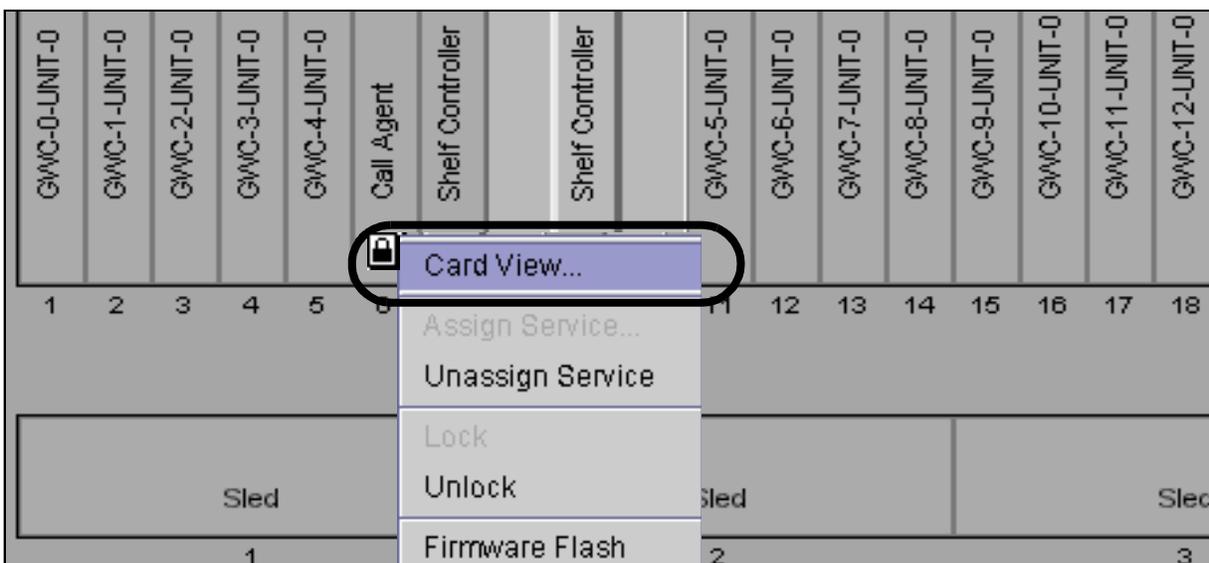
At the CS 2000 SAM21 Manager client workstation

- 1 Right-click on the card icon in the Shelf View and select Lock from the context menu.

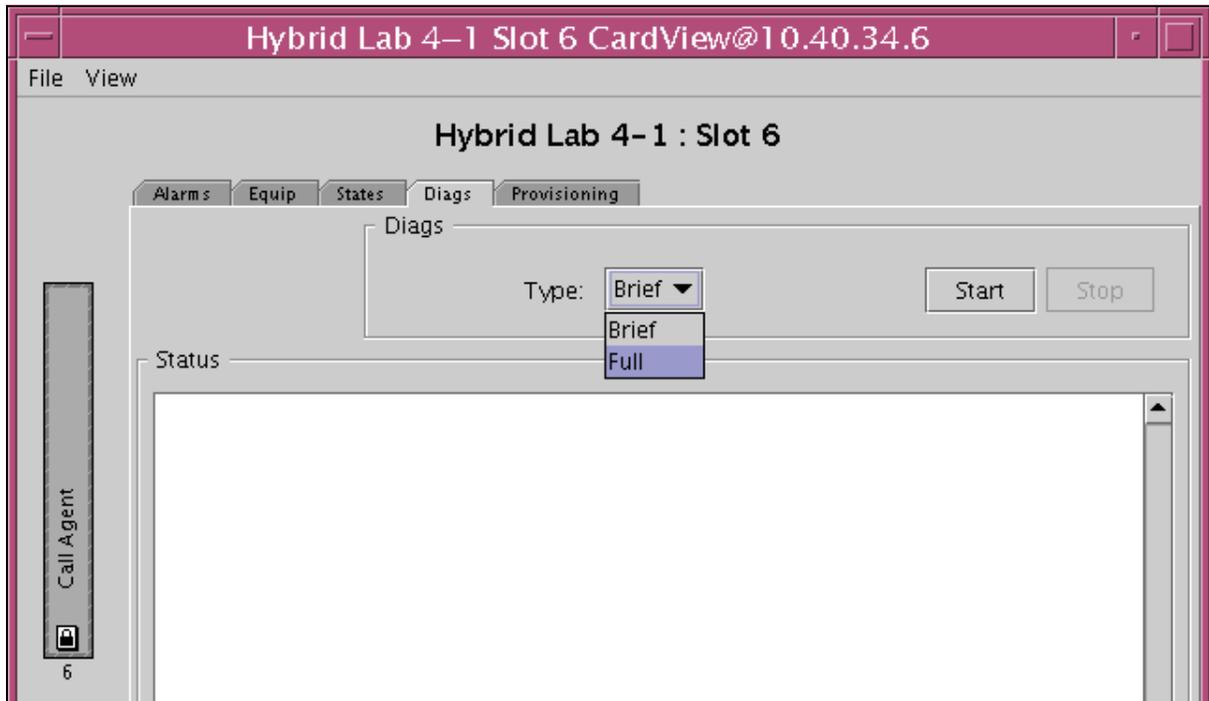


Note: Lock is also available from the States tab of the Card View window.

- 2 Right-click on the card icon in the Shelf View and select Card View from the context menu to open the Card View window.



- 3 Click on the Diagnostics tab from the Card View.

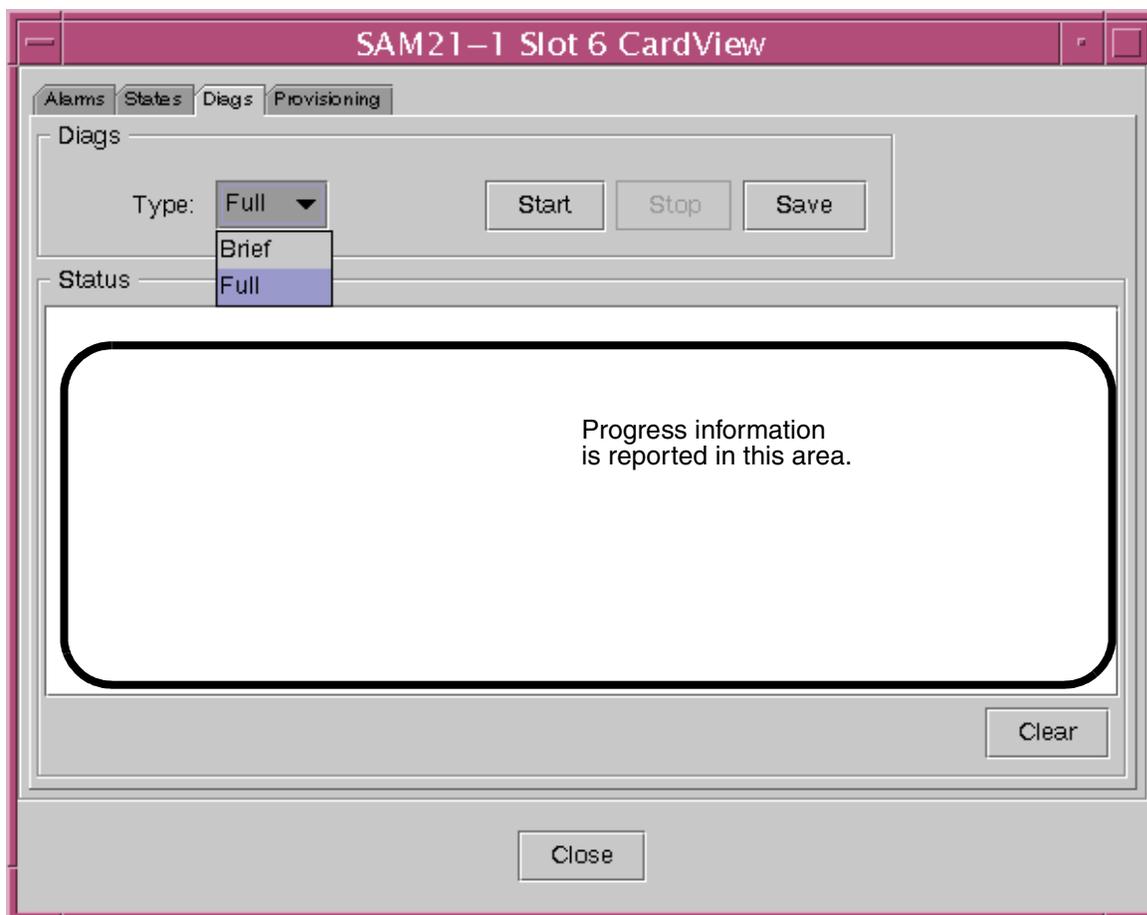


- 4 Select Brief or Full from the Type drop down menu and click on the Start button.
A confirmation dialog appears. Confirm the dialog.
- 5 Optionally monitor diagnostics. Refer to procedure [Monitoring diagnostics on page 177](#).
If diagnostics do not report “succeed!”, retry brief diagnostics and then full diagnostics. If either retry fails, replace the card.
- 6 After diagnostics complete, unlock the card from the Shelf View.
- 7 This procedure is complete.

Monitoring diagnostics

At the CS 2000 SAM21 Manager client workstation

- 1 Monitor the progress of the diagnostics from the Diags panel of the Card View.



- 2 Determine the next action:

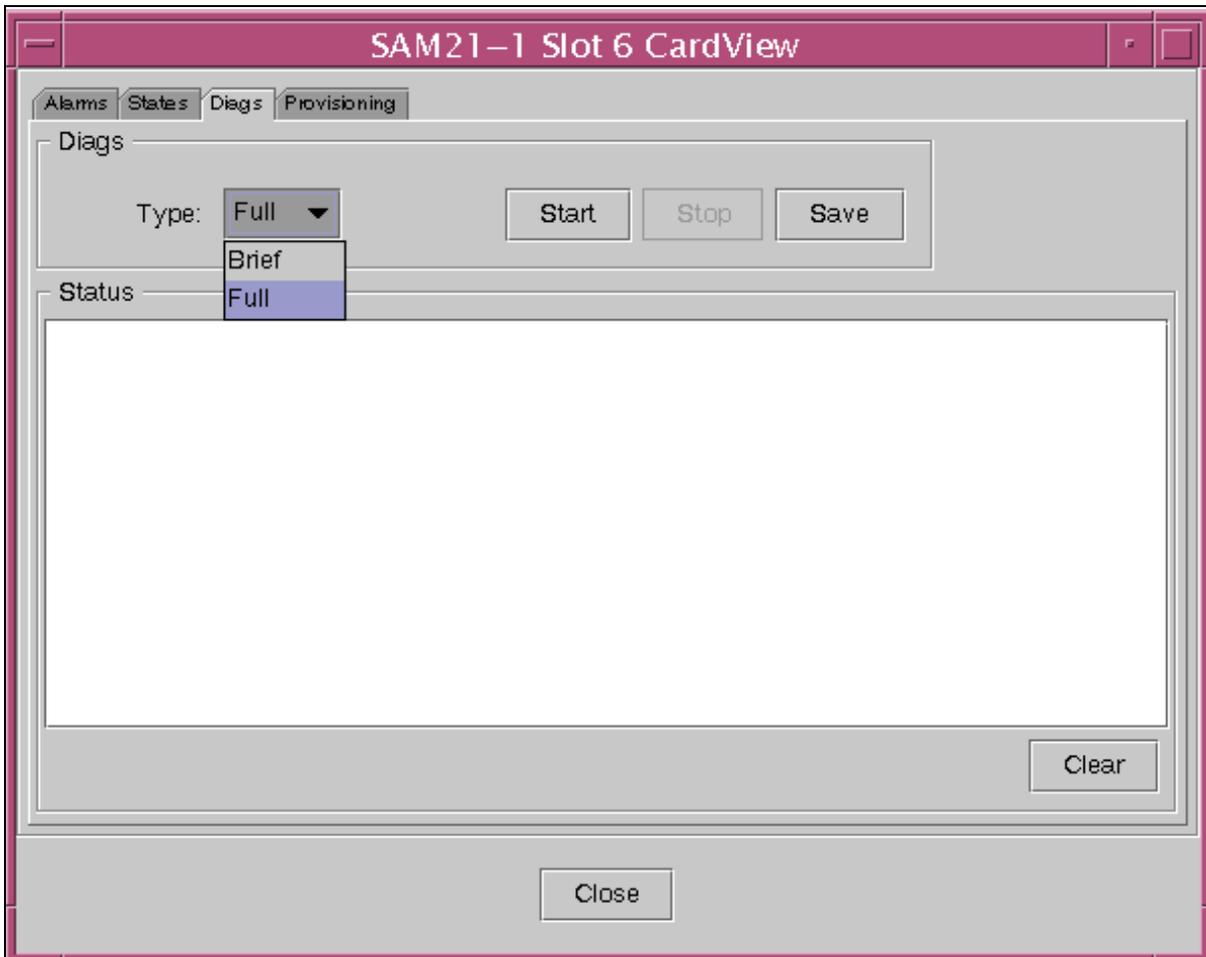
| If | Do |
|-------------------------------------|---|
| diagnostics report "Success" | Optionally save the diagnostics by using the Save button. Otherwise, take no action. |
| diagnostics do not report "Success" | Try brief diagnostics and then full diagnostics. If either diagnostic fails, replace the card and contact Nortel support. |

- 3 This procedure is complete.

Aborting diagnostics

At the CS 2000 SAM21 Manager client workstation

- 1 While diagnostics are in progress, click the Stop button from the Card View window.



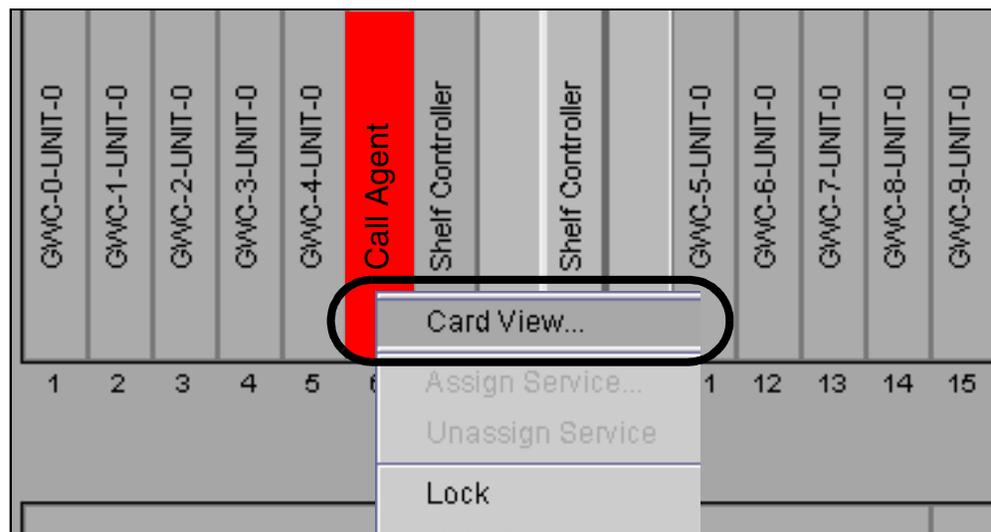
- 2 Unlock the card from the Shelf View.
- 3 This procedure is complete.

Retrieving alarms

Use this procedure to determine hardware, firmware, and other platform alarms. Call processing application alarms are not available from the CS 2000 SAM21 Manager.

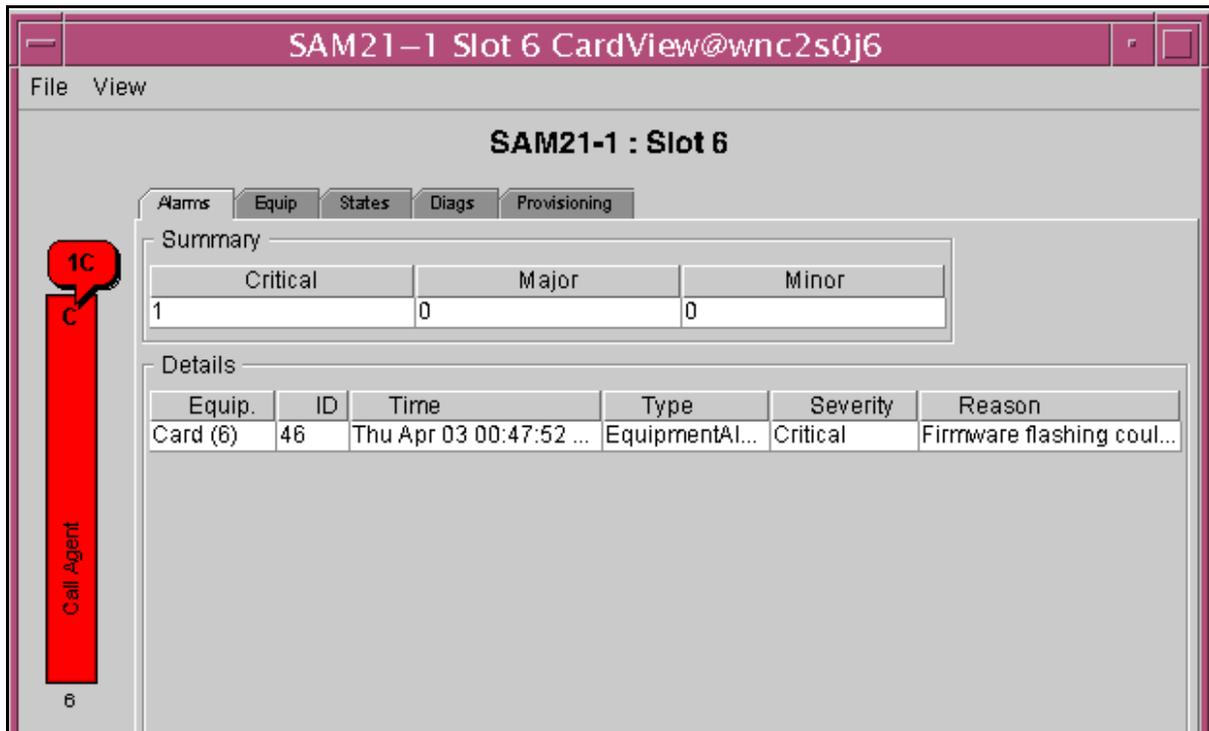
At the CS 2000 SAM21 Manager client workstation

- 1 Right-click on the card icon and select Card View from the context menu to open the Card View window.



Note: Alarms may disappear during recovery activities because automatic recovery of cards in the shelf is the responsibility and default behavior of the SAM21 Shelf Controller.

- 2 Click the Alarms tab on the Card View window.



The screenshot shows a window titled "SAM21-1 Slot 6 CardView@wnc2s0j6". The window has a menu bar with "File" and "View". Below the menu bar, the title "SAM21-1 : Slot 6" is displayed. There are five tabs: "Alarms", "Equip", "States", "Diags", and "Provisioning". The "Alarms" tab is selected. A red callout box with the number "1C" and a speech bubble icon points to the "Alarms" tab. Below the tabs, there is a "Summary" section with a table:

| Critical | Major | Minor |
|----------|-------|-------|
| 1 | 0 | 0 |

Below the summary is a "Details" section with a table:

| Equip. | ID | Time | Type | Severity | Reason |
|----------|----|-------------------------|----------------|----------|---------------------------|
| Card (6) | 46 | Thu Apr 03 00:47:52 ... | EquipmentAl... | Critical | Firmware flashing coul... |

On the left side of the window, there is a vertical red bar with the text "Call Agent" and the number "6" at the bottom.

- 3 This procedure is complete.

Additional information

The following table indicates alarm types and possible actions to take.

Alarm codes

| Alarm ID | Severity | Remedy |
|----------|----------|--|
| 15 | Major | <p>Use the alarm text to determine which condition exists.</p> <ul style="list-style-type: none"> • Diagnostic failed at test case Rerun diagnostics. If diagnostics fail a second time, replace the card. If no Field Replaceable Units (FRU) are available, contact Nortel support personnel. • Diagnostics failed due to SWACT Rerun diagnostics. • Diagnostics failed, <msg> <i>where</i> <msg> is one of the following: <ul style="list-style-type: none"> — due to Software error — no such device — board in wrong state — could not connect to board — terminated by unexpected timeout — terminated unexpectedly — at test case — terminated by user Rerun diagnostics. If diagnostics fail a second time, replace the card. • Unknown failure, board is not accessible Rerun diagnostics. If diagnostics fail a second time, replace the card. |

Alarm codes

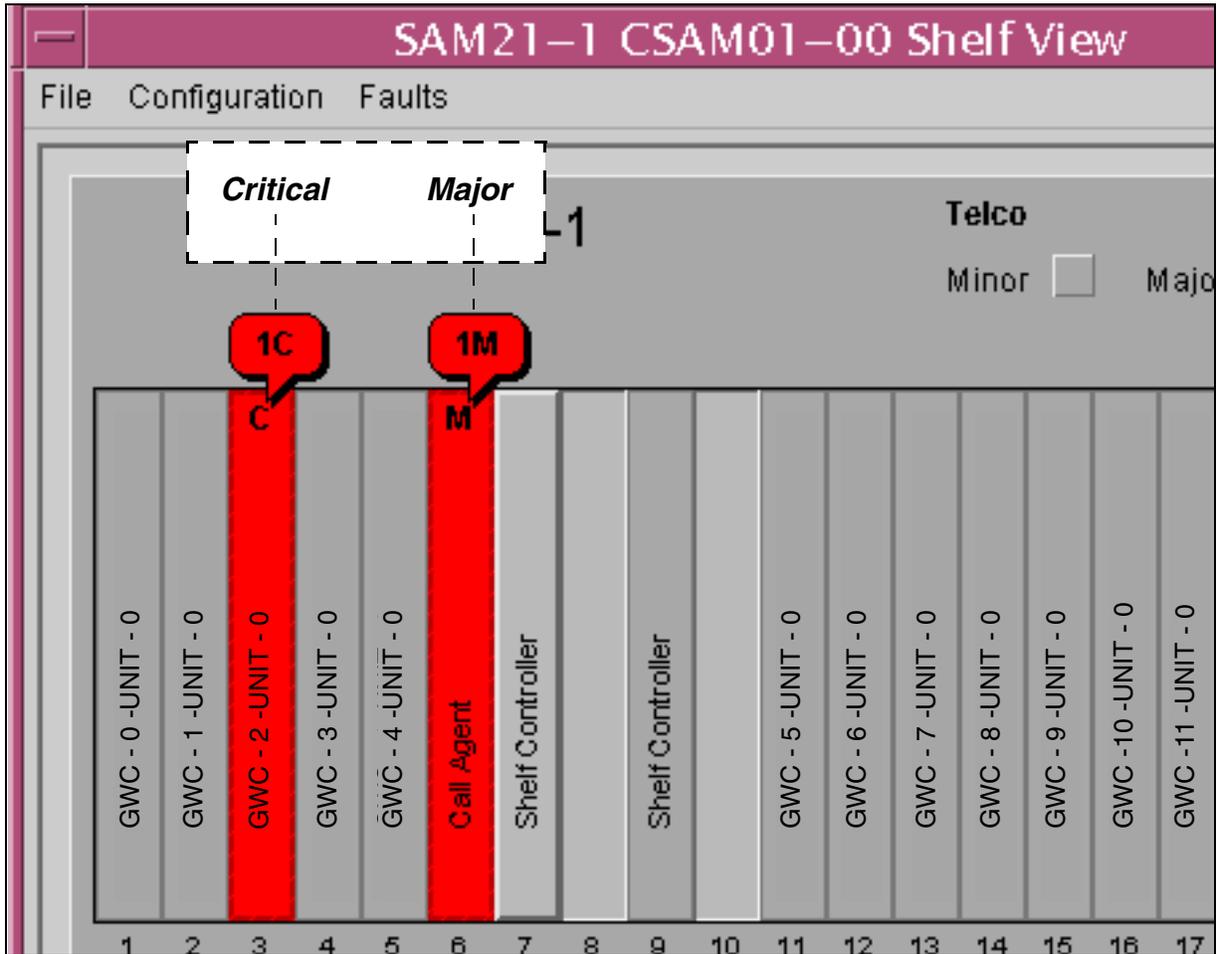
| Alarm ID | Severity | Remedy |
|----------|----------|--|
| 46 | Critical | <p>Use the alarm text to determine which condition exists.</p> <ul style="list-style-type: none">Firmware flashing could not connect to the board Resend provisioning data from the Provisioning tab of the Card View window. Note: Auto Flash is now disabled for cards in this slot. Optionally re-enable Auto Flash on the Provisioning tab.Firmware flashing failed at downloading firmware Verify that the component software fileset is installed and APPLIED on the SWIM level of the Preside CS 2000 Core Manager. Resend the provisioning data from the Provisioning tab of the Card View window.Firmware flashing failed at validating firmware The firmware file is corrupt or was corrupted in transfer. Verify that the component software fileset is installed and APPLIED at the SWIM level of the Preside CS 2000 Core Manager. Resend the provisioning data from the Provisioning tab of the Card View window.Firmware flashing failed at backing up firmware If condition persists, replace the card.Firmware flashing failed flash The card was inaccessible after the flash. Reseat the card and try again. If the problem persists, replace the card. Note: Auto Flash is now disabled for cards in this slot. Optionally re-enable Auto Flash on the Provisioning tab. |

Alarm codes

| Alarm ID | Severity | Remedy |
|----------|----------|--|
| | | <ul style="list-style-type: none"> Firmware flash failed <msg> <i>where</i> <msg> is one of the following: <ul style="list-style-type: none"> — due to a software error — no such device — board in wrong state — terminated by unexpected timeout — board is not accessible — terminated <p>Resend the provisioning data from the Provisioning tab of the Card View window. If this problem persists, replace the card.</p> |
| 48 | Critical | <ul style="list-style-type: none"> Provision failed: process ended abnormally Provision failed, could not connect to board Provision failed to set application type <p>Resend the provisioning data from the Provisioning tab of the Card View window. If the problem persists and is isolated to this card, replace the card.</p> <p>If the problem affects more than one card, verify cabling, fileset installation at the SWIM level of the CS 2000 Core Manager, and contact Nortel support personnel. If the CS 2000 Core Manager is not part of the network, verify that the host identified as the Server IP on the provisioning panel is in service and that the bootload specified in the Path and Load fields is available.</p> |

Refer to the following figure for information about how to determine alarm severity.

Alarm severity



Note: If the Call Agent card fails, the appearance is grey with a hashed outline.

Message controller procedures

When the CS 2000 - Compact is deployed in a Time Division Multiplex (TDM) network, a pair of Message Controller cards are installed in the SAM21 shelf. These cards work between the Call Agent cards and the Message Switch (MS).

Fault management strategy

Fault management for the Message Controller is completed through the Call Agent Manager and the CS 2000 SAM21 Manager. The Call Agent Manager controls in service maintenance activities and the CS 2000 SAM21 Manager controls out of service maintenance activities.

Call Agent Manager with Message Controller cards

```

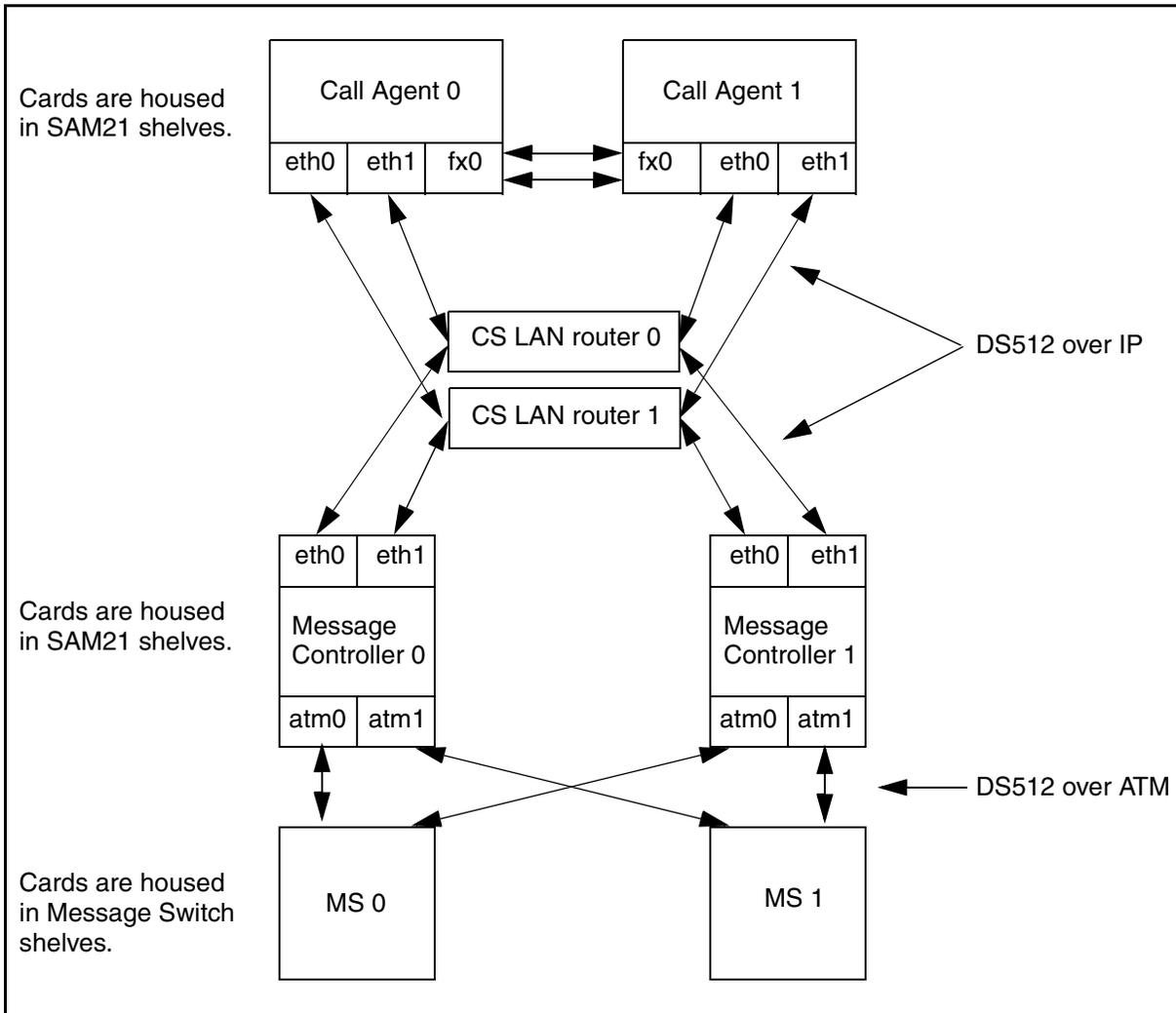
CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .              .              .              .

CCAMtc
0 Quit
2 CoreMtc
3 Admin
4
5
6
7 MCMtc
8
9
10
11          MCMtc:      Enter the MC blade maintenance level.
12                                The following activities can be performed under the
13 LogQuery                                maintenance level:
14 Alarm          - monitor overall system state and alarms
15                                - display link hit rate on an MC blade
16                                - clear hit rate on an MC blade
17 Help          - display relationship between ATM links and MC
18 Refresh      - display MC blade load version
          mtc
Time 08:13 >
    
```

Connectivity

Link connectivity among Call Agent cards, the Message Controller cards, and the CMIC cards in the Message Switch (MS) are indicated in the figure below.

Message Controller messaging connectivity



Eth0 and eth1 physical interfaces are implemented in software as virtual and redundant Ethernet links. CS LAN routers use virtual router redundancy protocol (VRRP) for reliability. DS512 is a proprietary signalling format used for messaging between the call processing application running on the Call Agent cards and the Message Switch. ATM interface ports are not represented in the figure because different CMIC cards on the Message Switch offer different numbers of ports.

ATM links from Message Controller cards to CMIC card ports on the Message Switch are configured according to the office configuration. Refer to the following table for SuperNode (SN) and SN Size Enhanced (SNSE) configurations.

| | SN | | | | SNSE | | | |
|-----------------------------|----|----|----|----|------|---|---|---|
| Message Controller | 0 | | 1 | | 0 | | 1 | |
| Message Controller ATM port | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| MS port | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| MS card | 24 | 25 | 25 | 24 | 4 | 4 | 4 | 4 |
| MS | 0 | | 1 | | 0 | | 1 | |

The TRNSL command reports this information from the Call Agent Manager and Shelf and Card sublevels of the MS level on the MAP.

Trns1 from Call Agent Manager

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        .

MCMtc          Blade:   Eth0:    Eth1:    Atm0:    Atm1:
0 Quit         MC0     .        . Act    . Inact  open     open
2              MC1     .        . Act    . Inact  open     open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trns1
9
10
11             Connectivity report for MC0 retrieved on:
12             Fri Apr 4 09:44:19 2003
13 LogQuery
14 Alarm
15
16             MS      Card  Port  Cod  Connection
17             -----
18 Help        ATM0 connected to: 0      24   0    NO   GOOD
19 Refresh     ATM1 connected to: 1      25   0    NO   GOOD
    mtc
Time 09:44 > Trns1 0

```


State information from Call Agent Manager

```

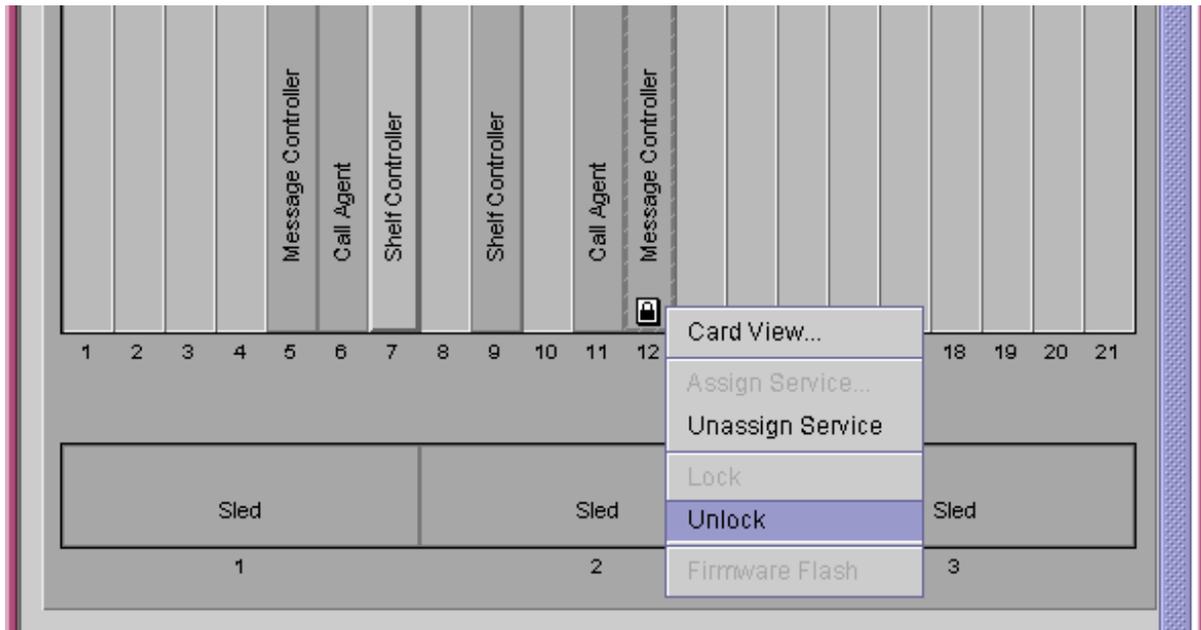
CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        .
MCMtc
0 Quit        MC0      .        . Act    . Inact  open    open
2              MC1      .        . Act    . Inact  open    open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
   mtc
Time 09:44 >

```

- . - in service
The Message Controller is in service.
- S - system busy
This Message Controller does not have connectivity to either Call Agent unit. Investigate Ethernet link pulls or CS LAN router misconfiguration.
- R - remote busy
This Message Controller was locked from the CS 2000 SAM21 Manager. When the Message Controller is unlocked from the CS 2000 SAM21 Manager, the state transitions to in service.

The state of the card is also available from the CS 2000 SAM21 Manager.

Message Controller at CS 2000 SAM21 Manager



The States tab, available from the Card View window, provides information about the state of the Message Controller. For information about diagnosing the state of the Message Controller from the card icons displayed at the CS 2000 SAM21 Manager, refer to [Card icons](#).

Message Controller card replacement

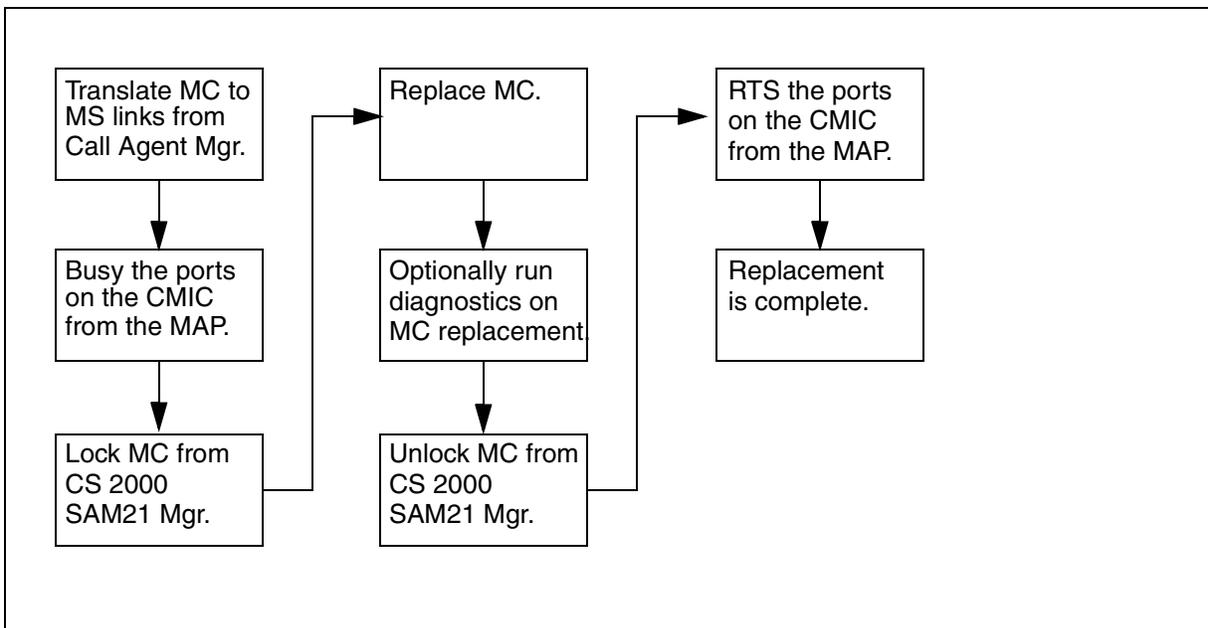


CAUTION

Possible service interruption

Only perform this procedure at the direction of Nortel support personnel.

The following figure summarizes the steps required to replace a Message Controller card.



The following variables are used in this procedure.

| Variable | Where determined | Where used |
|----------|--|--|
| mc_no | This is the Message Controller card number to replace, 0 or 1. Support personnel determine which Message Controller to replace. | Step 1 . |
| card_no | This is the CMIC card number on the Message Switch. It is determined from the output in step 1 . If the office is in a SuperNode (SN) configuration, the card_no is either 24 or 25. If the office is in a SN Size Enhanced (SNSE) configuration, then card_no is 4. | Steps 2 and 16 . |

| Variable | Where determined | Where used |
|----------|--|--|
| ms_no | This is the Message Switch number, 0 or 1. Both are used, but the ms_no, card_no, and port_no combinations reported in step 1 identify unique links. | Steps 2 and 16 . |
| port_no | This identifies the ATM link between a port on the CMIC card in the Message Switch and one of the two ATM interfaces on the Message Controller faceplate. Two port numbers are used, 0 and 1. It is determined from the output in step 1 . | Steps 2 and 16 . |

At the Call Agent Manager

- 1 Enter the MCMtc level and translate the Message Controller links back to the CMIC card in the Message Switch shelf.

MCMtc

Trns1 <mc_no>

**Example
Trns1 0**

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .              .              .              .

MCMtc          Blade:   Eth0:      Eth1:      Atm0:     Atm1:
0 Quit        MC0      .          . Act      . Inact   mtc open  closed
2             MC1      .          . Act      . Inact   open      open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trns1       Connectivity report for MC0 retrieved on:
9             Tue Mar 11 10:37:22 2003
10
11
12
13 LogQuery   -----
14 Alarm      ATM0 connected to:  0      4      0      NO      GOOD
15           ATM1 connected to:  1      4      1      NO      GOOD
16
17 Help
18 Refresh
   mtc
Time 10:37 >Trns1 0

```

These are the two ms_no, card_no, and port_no combinations needed.

At the MAP

- 2 Enter the MS level and busy the two ports identified in [step 1](#).

```
>MAPCI;MTC;MS;SHELF 0;CARD <card_no>;
BSY <ms_no> PORT <port_no>
```

Example

```
>CARD 4; BSY 0 PORT 0
>CARD 4; BSY 1 PORT 1 FORCE
```

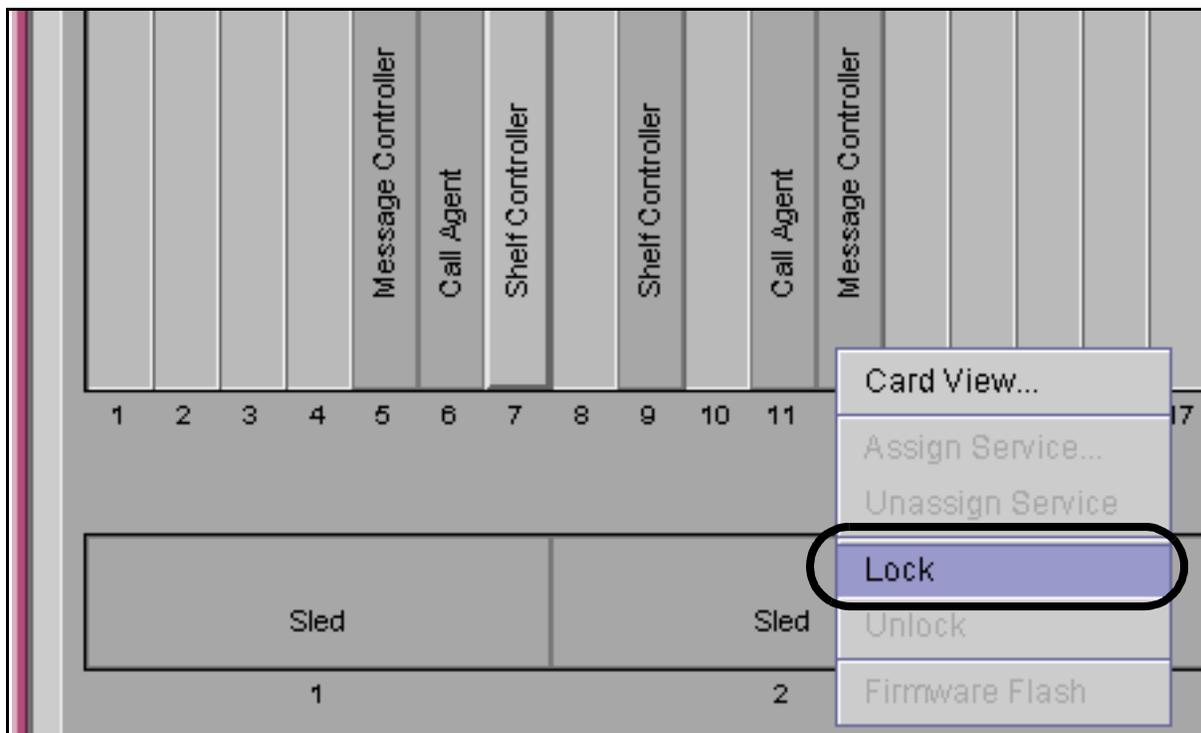
Both ATM links to the Message Controller are set to manual busy. Two CMIC alarms, "02CMIC" are raised at the MAP and a major ATM alarm is raised at the Call Agent Manager. Two MS301 log reports and two CCA340 log reports are generated.

```

      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
      02CMIC      .      .      .      .      .      .      .      .
CARD
      Message Switch      Clock      Shelf      0      Inter-MS Link 0 1
0 Quit      MS 0      .      Master      F      . .
2      MS 1      .      Slave      F      . .
3
4      Shelf 0      1 1 1 1
5      Card 1 2 3 4 5 6 7 8 9 0 1 2 3
6 Tst_      Chain      |      |
7 Bsy_      MS 0      . . . F - . - - . . - .
8 RTS_      MS 1      . . . F - . - - . . - .
9 Offl_
10      Card 04 CMIC Interface Card      Port: 0 1
11 LoadCd_      MS 0      .      M .
12 QueryCd_      MS 1      .      . M
13 Card_
14 QueryMS
15 Trnsl_
16
17 Next
18 Port_
      MIKEM
Time 11:39 >CARD 4; BSY 0 PORT 0; CARD 4; BSY 1 PORT 1 FORCE
```

At the CS 2000 SAM21 Manager client workstation

- 3 From the Shelf View, right click on the card and select Lock from the context menu.



The Message Controller is removed from service. No new alarms are raised at the MAP. The Call Agent Manager reports the card as "blade out-of-service." An SCU500 log report is generated by the SAM21 Shelf Controller to indicate the state change to locked-disabled-none.

- 4 Wait for the lock icon to appear on the selected card.

At the SAM21 frame

- 5 Label and remove the fiber connections from the faceplate.
- 6 Open the bottom ejector lever.
Note: Wait for the green LED on the faceplate to extinguish and a blue LED to light at the bottom of the faceplate.
- 7 Wait for the blue LED to appear at the bottom of the faceplate and the red out-of-service LED above the card to extinguish.
- 8 Press both ejector levers until the card is ejected from the shelf.

9

**CAUTION****Possible service interruption**

A service outage can occur if care is not taken while inserting the circuit pack.

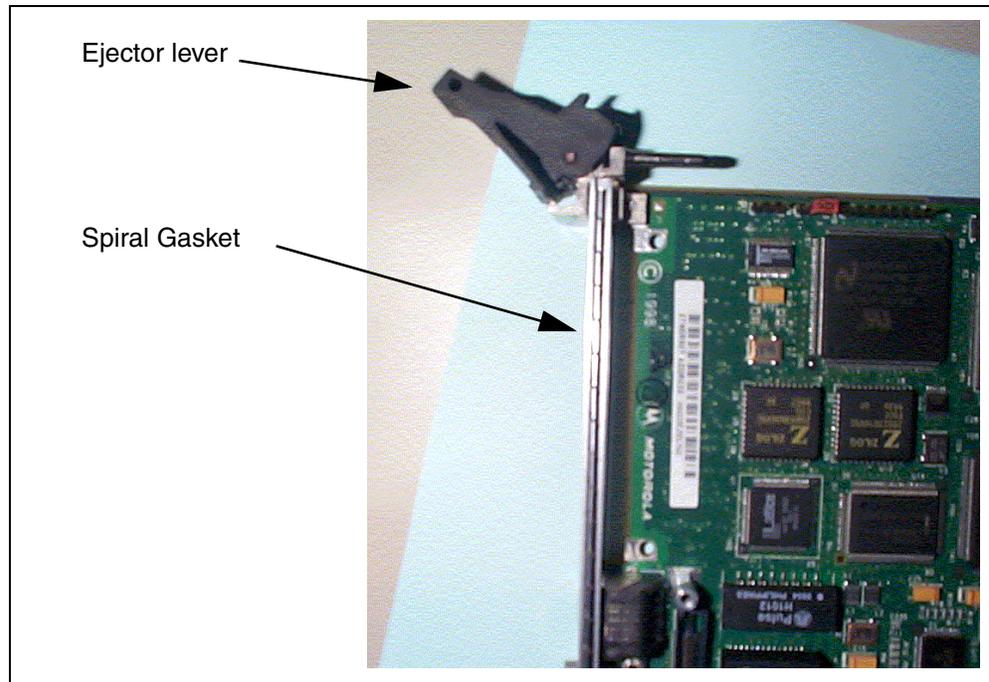
The spiral gasket, located on the faceplate of the circuit pack, can become caught on an adjacent card and ripped off of the faceplate. If the spiral gasket ends up making contact with the backplane inside the chassis, an electrical short circuit can result in a service outage.

**WARNING****Static electricity damage**

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the SAM21 Shelf Cabinet when handling the replacement card. This protects the card against damage caused by static electricity.

Hold the replacement card by the ejector levers and remove the card from the shelf.

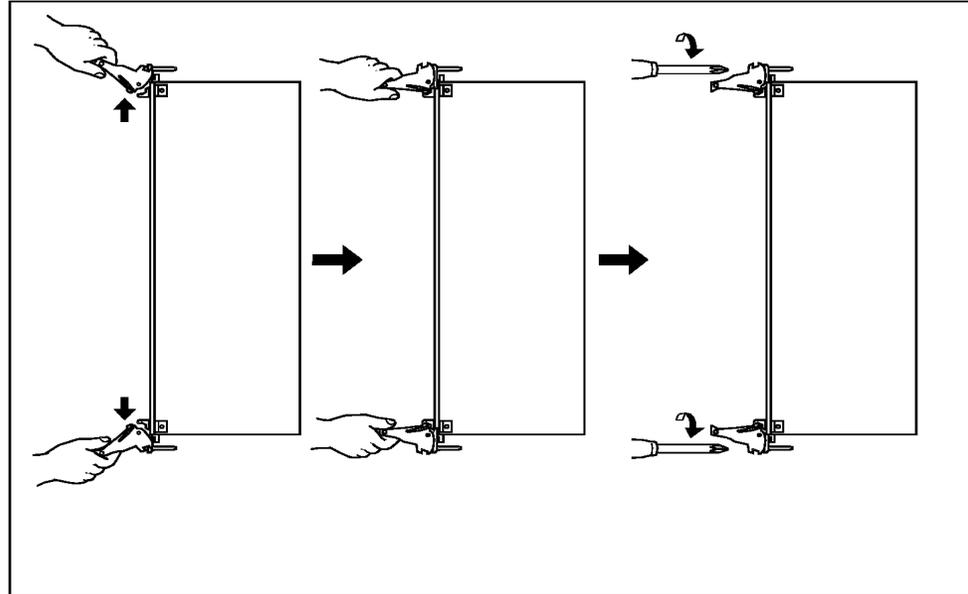
- 10 Examine the circuit packs before inserting them in the SAM21 chassis to ensure that the spiral gasket is seated and not loose.



- 11 Hold the replacement card by the ejector levers and insert the card into the shelf.

Note 1: Do not push on the faceplate to seat the card.

Note 2: Verify that the CPU LED lights. If the CPU LED does not light, reset the card. If the CPU LED fails to light a second time, replace the card.



- 12 Secure the board by tightening the captive screws at the top and bottom of the panel.
- 13 Reconnect the fiber connections to the faceplate.

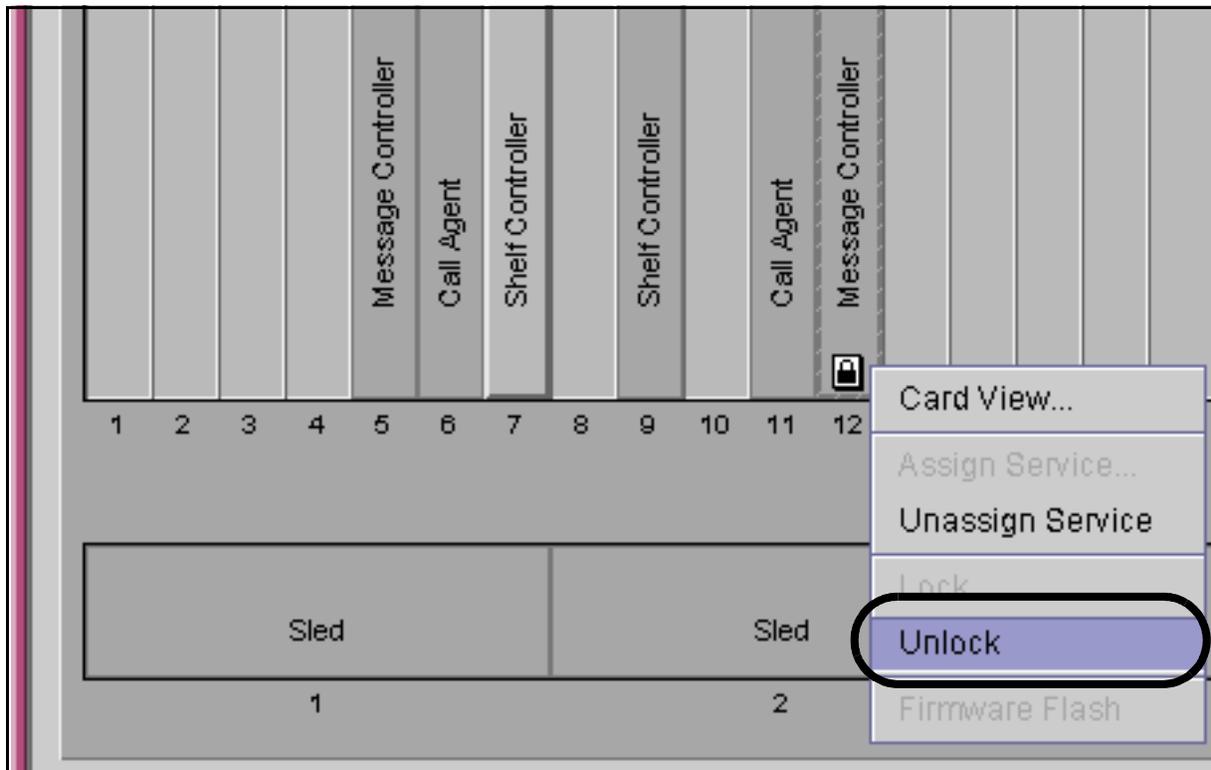
At the CS 2000 SAM21 Manager client workstation

- 14 Optionally run brief diagnostics on the replacement card. Refer to procedure [Running diagnostics](#).
- 15 Right click on the card icon and select Unlock from the Shelf View. Optionally monitor the download from the States tab of the Card View window.

Wait for the lock icon to disappear from the card on the Shelf View. An SCU500 log report is generated by the SAM21

Shelf Controller to record the state change to unlocked-enabled-none.

At the Call Agent Manager, the Message Controller transitions from offline to in service and the ATM alarm clears. Two CCA640 log reports are generated.



At the MAP

- 16** Return to service the ports that were busied.

>CARD <card_no>; RTS <ms_no> PORT <port_no>

Example

>CARD 4; RTS 0 PORT0; CARD 4; RTS 1 PORT 1

The ports change state from manual busy (M) to in service (.) and the CMIC alarms clear from the MS area of the alarm banner. At the Call Agent Manager, the ATM ports transition from

open, to maintenance open, and back to open. Two MS300 log reports are generated.

```

      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
      .      .      .      .      .      .      .      .      .

CARD
0 Quit      MS 0      .      .      .      .      .      .      .
2          MS 1      .      .      .      .      .      .      .
3
4          Shelf 0      .      .      .      .      .      .      .
5          Card 1 2 3 4 5 6 7 8 9 0 1 2 3
6 Tst_      Chain      |      |
7 Bsy_      MS 0      . . . . - . - - . . - .
8 RTS_      MS 1      . . . . - . - - . . - .
9 Offl_
10         Card 04 CMIC Interface Card      Port: 0 1
11 LoadCd_  MS 0      .      .      .
12 QueryCd_ MS 1      .      .      .
13 Card_
14 QueryMS
15 Trnsl_
16
17 Next
18 Port_
  MIKEM
Time 11:39 >RTS 0 PORT 0; RTS 1 PORT 1

```

17 This procedure is complete.

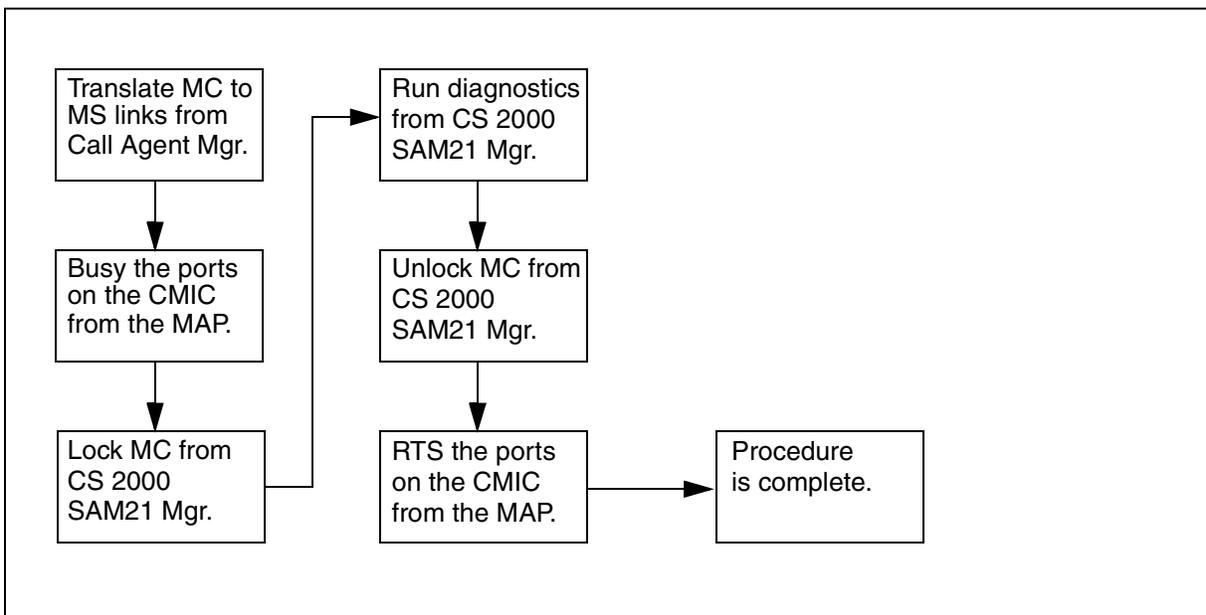
Running diagnostics

ATTENTION

Running diagnostics on a Message Controller card requires removing the Message Controller from service. Redundant operation of the Message Controllers is lost until the Message Controller is returned to service.

The following figure summarizes the steps required to run diagnostics on a Message Controller card.

Summary of running diagnostics on a Message Controller card



The following variables are used in this procedure.

| Variable | Where determined | Where used |
|----------|---|---|
| mc_no | This is the Message Controller card number on which to run diagnostics, 0 or 1. Support personnel determine the Message Controller on which to run diagnostics. | Steps 1 and 9 . |
| card_no | This is the CMIC card number on the Message Switch. It is determined from the output in step 1 . If the office is in a SuperNode (SN) configuration, the card_no is either 24 or 25. If the offices is in a SN Size Enhanced (SNSE) configuration, then card_no is 4. | Steps 2 and 9 . |
| ms_no | This is the Message Switch number, 0 or 1. Both are used, but the ms_no, card_no, and port_no combinations reported in step 1 identify unique links. | Steps 2 and 9 . |
| port_no | This identifies the ATM link between a port on the CMIC card in the Message Switch and one of the two ATM interfaces on the Message Controller faceplate. Two port numbers are used, 0 and 1. It is determined from the output in step 1 . | Steps 2 and 9 . |

At the Call Agent Manager

- 1 Enter the MCMtc level and translate the Message Controller links back to the CMIC card in the Message Switch shelf.

MCMtc

Trns1 <mc_no>

**Example
Trns1 0**

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .              .              .              .
MCMtc          Blade:   Eth0:      Eth1:      Atm0:    Atm1:
0 Quit        MC0      .          . Act      . Inact   mtc open  closed
2             MC1      .          . Act      . Inact   open      open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trns1       Connectivity report for MC0 retrieved on:
9             Tue Mar 11 10:37:22 2003
10
11
12
13 LogQuery   -----
14 Alarm      ATM0 connected to: 0  4  0  NO  GOOD
15           ATM1 connected to: 1  4  1  NO  GOOD
16
17 Help
18 Refresh
   mtc
Time 10:37 >Trns1 0

```

These are the two ms_no, card_no, and port_no combinations needed.

At the MAP

- 2 Enter the MS level and busy the two ports identified in [step 1](#).

```
>MAPCI;MTC;MS;SHELF 0;CARD <card_no>;
BSY <ms_no> PORT <port_no>
```

Example

```
>CARD 4; BSY 0 PORT 0
>CARD 4; BSY 1 PORT 1 FORCE
```

Both ATM links to the Message Controller are set to manual busy. Two CMIC alarms, "02CMIC" are raised at the MAP and a major ATM alarm is raised at the Call Agent Manager. Two MS301 log reports and two CCA340 log reports are generated.

```

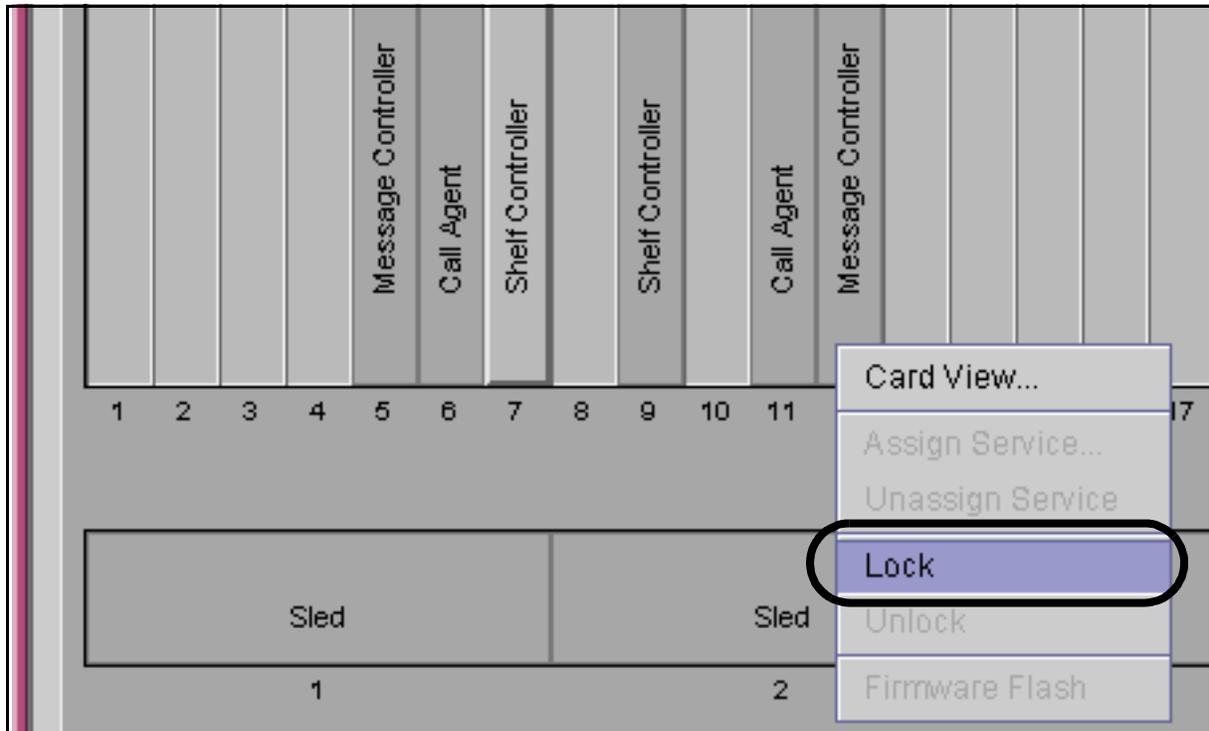
      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
02CMIC      .          .          .          .          .          .          .          .

CARD
0 Quit      MS 0      .          Master      F          .          .          .
2          MS 1      .          Slave       F          .          .          .
3
4          Shelf 0      .          .          .          .          .          .          .
5          Card 1 2 3 4 5 6 7 8 9 0 1 2 3
6 Tst_      Chain          |          |
7 Bsy_      MS 0      . . . F - . - - . . .
8 RTS_      MS 1      . . . F - . - - . . .
9 Offl_
10         Card 04 CMIC Interface Card      Port: 0 1
11 LoadCd_  MS 0      .          .          M .
12 QueryCd_ MS 1      .          .          . M
13 Card_
14 QueryMS
15 Trnsl_
16
17 Next
18 Port_
MIKEM
Time 11:39 >CARD 4; BSY 0 PORT 0; CARD 4; BSY 1 PORT 1 FORCE

```

At the CS 2000 SAM21 Manager client workstation

- 3 From the Shelf View, right click on the card and select Lock from the context menu.

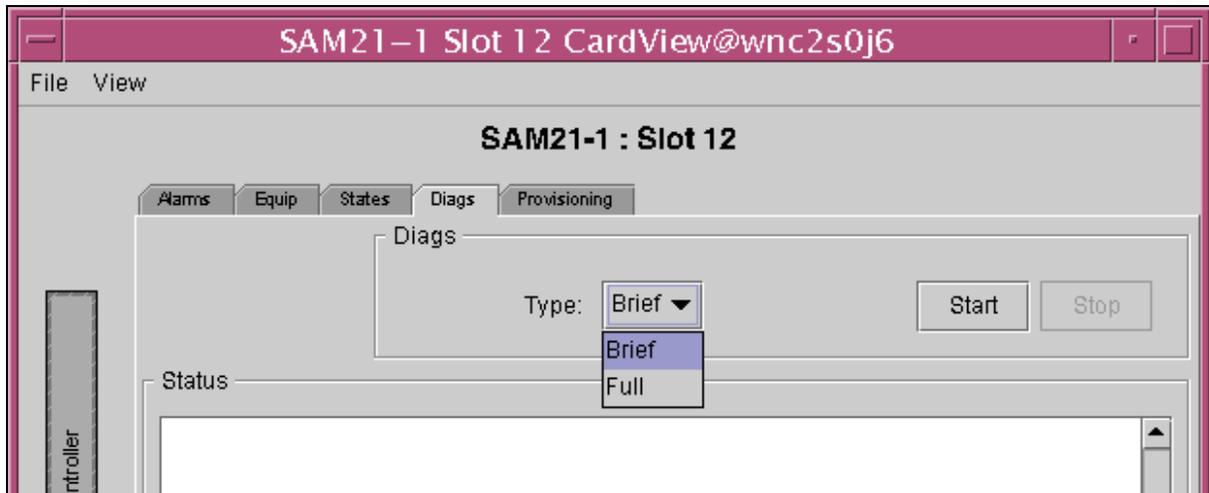


The Message Controller is removed from service. No new alarms are raised at the MAP. The Call Agent Manager reports the card as "blade out-of-service." An SCU500 log report is generated by the SAM21 Shelf Controller to indicate the state change to locked-disabled-none.

- 4 Wait for the lock icon to appear on the selected card.
- 5 Right-click on the card icon and select Card View from the card context menu.

The Card View window for the Message Controller opens.

- 6 Click the Diags tab on the Card View window. Select full or brief diagnostics and then click Start.



A confirmation dialog window opens.

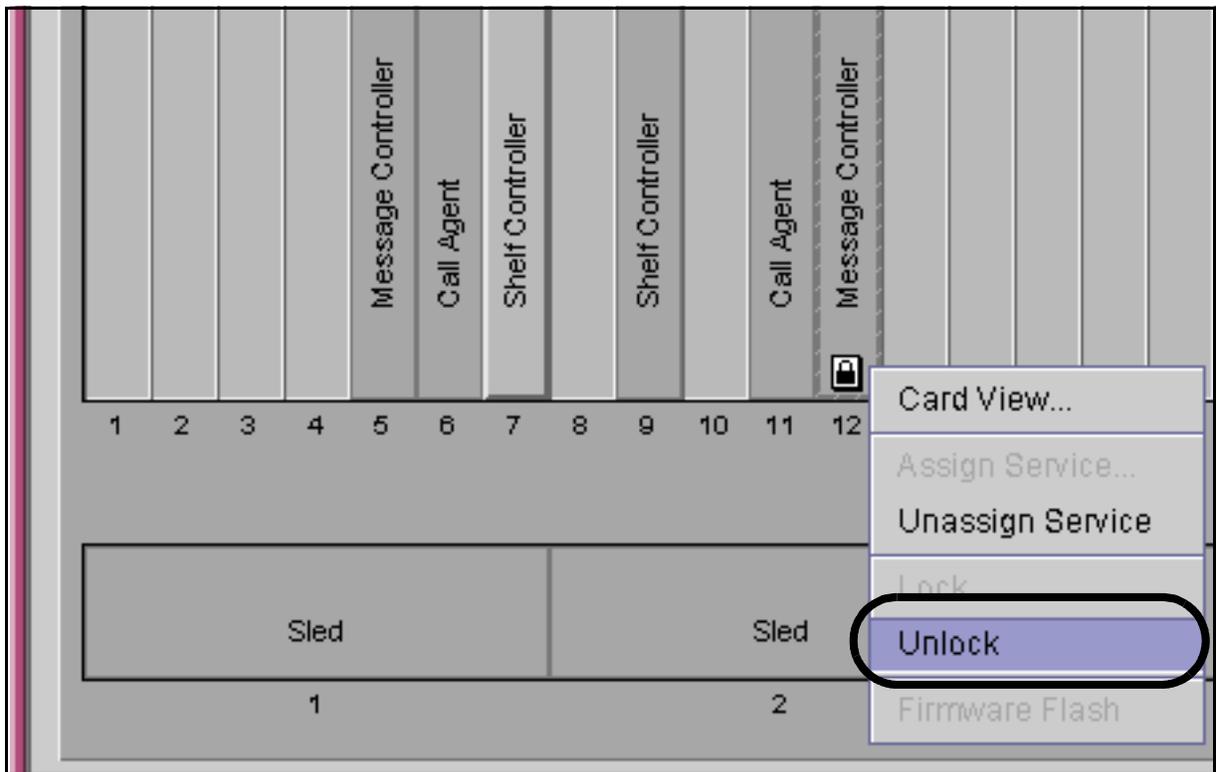
- 7 Confirm the diagnostics and then monitor the diagnostics in the Status window. After diagnostics complete, optionally save the results to the local workstation.

If diagnostics fail, retry brief and then full diagnostics. If either run fails, save the results and replace the card. Contact Nortel support personnel for assistance.

- 8 Right click on the card icon and select Unlock from the Shelf View. Optionally monitor the download from the States tab of the Card View window.

Wait for the lock icon to disappear from the card on the Shelf View. An SCU500 log report is generated by the AM21 Shelf Controller to record the state change to unlocked-enabled-none.

At the Call Agent Manager, the Message Controller transitions from offline to in service and the ATM alarm clears. Two CCA640 log reports are generated.



At the MAP

9 Return to service the ports that were busied.

>CARD <card_no>; RTS <ms_no> PORT <port_no>

Example

>CARD 4; RTS 0 PORT0; CARD 4; RTS 1 PORT 1

The ports change state from manual busy (M) to in service (.) and the CMIC alarms clear from the MS area of the MAP alarm banner. At the Call Agent Manager, the ATM ports transition from open, to maintenance open, and back to open. Two MS300 log reports are generated.

```

      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
      .      .      .      .      .      .      .      .      .
CARD
      Message Switch      Clock      Shelf 0      Inter-MS Link 0 1
0 Quit      MS 0      .      Master      .      .
2      MS 1      .      Slave      .      .
3
4      Shelf 0      1 1 1 1
5      Card 1 2 3 4 5 6 7 8 9 0 1 2 3
6 Tst_      Chain      |      |
7 Bsy_      MS 0      . . . . - . - - . . - .
8 RTS_      MS 1      . . . . - . - - . . - .
9 Offl_
10      Card 04 CMIC Interface Card      Port: 0 1
11 LoadCd_  MS 0      .
12 QueryCd_ MS 1      .
13 Card_
14 QueryMS
15 Trnsl_
16
17 Next
18 Port_
      MIKEM
Time 11:39 >RTS 0 PORT 0; RTS 1 PORT 1

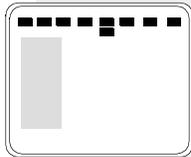
```

10 This procedure is complete.

MC ATM

minor, major or critical

Alarm display



| | | | | | |
|-----------|-----|-----|------|-----|---------|
| CallAgent | SYS | CON | APPL | MC | Unit: 0 |
| . | . | . | . | ATM | |

Indication

A CCA340 log report is generated when the alarm is raised. A CCA640 log report is generated when the alarm clears.

Meaning

A minor severity alarm indicates that 1 or 2 ATM links are down, but that no Message Controller is isolated. Call processing is not affected. When the Message Switch executes a routine exercise test (REx), two ATM ports are set to maintenance open and a minor ATM alarm is raised.

A major severity alarm indicates that a Message Controller is isolated. Call processing is not affected.

A critical severity alarm indicates that all ATM links are down. Call processing is interrupted.

Action

At the Call Agent Manager

- 1 Enter the MCMtc level.

MCMtc

- 2 Determine the link status.

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        ATM
MCMtc
0 Quit        MC0      .        . Inact   . Act
2             MC1      .        . Inact   . Act
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
   mtc
Time 13:12 >

```

| Blade: | Eth0: | Eth1: | Atm0: | Atm1: |
|--------|---------|-------|-------|--------|
| . | . Inact | . Act | open | closed |
| . | . Inact | . Act | open | open |

open - the ATM link is available
 closed - the ATM link is down
 mtc open - the ATM link is under maintenance
 undetermined - the ATM link state is unknown

- 3 If two ports are in the maintenance open state, `mtc open`, determine if the Message Switch is executing a REX from the MAP. If so, the ATM alarm clears when the REX completes.
- 4 Translate the ATM link to the Message Switch (MS).

Trnsl <mc_no>

Example
Trnsl 0

The Message Switch number, card number, and port number are returned. Map the ATM ports in the closed state to the ms_no, card_no, and port_no on the Message Switch.

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        ATM
MCMtc
0 Quit        MC0      .        . Inact   . Act    Atm0:    Atm1:
2              MC1      .        . Inact   . Act    open     closed
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10
11             Connectivity report for MC0 retrieved on:
12             Mon Mar 10 13:53:16 2003
13 LogQuery
14 Alarm
15
16             MS      Card  Port  Cod  Connection
17             -----
18             ATM0 connected to: 0      24   0    NO   GOOD
19             ATM1 connected to: 1      25   0    NO   GOOD
    mtc
Time 13:53 > TRNSL 0
    
```

At the MAP

5 Enter the MS level.

>MAPCI;MTC;MS

6 Determine the correct MS shelf to use.

```

MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
01CMIC .        .        .        .        .        .        .        .        .

MS      Message Switch  Clock  Shelf  Inter-MS Link 0 1
0 Quit  MS 0              .      Slave  .        .
2       MS 1              .      Master F        .
3
4
5
6 Tst_
7 Bsy_
    
```

7 Use the Shelf command to enter the Shelf level.

>**SHELF** <shelf_no>

Example
>**SHELF 1**

8 Use the card number from [step 4](#) to view the card information.

>**CARD** <card_no>

Example
>**CARD 25**

9 Determine the state of the port.

```

MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
01CMIC .      .      .      .      .      .      .      .      .

MS      Message Switch      Clock      Shelf 0      Inter-MS Link 0 1
0 Quit      MS 0      .      Slave      .      .      .
2      MS 1      .      Master      F      .      .
3
4      Shelf 0      .      .      .      .      .      .      .      .      .      .      .      .      .      .      .      .
5      Card 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
6 Tst_      Chain      |      |
7 Bsy_      MS 0      . . . - . . - - - . - - - - - . - - - - - . . . . .
8 RTS_      MS 1      . . . - . . - - - . - - - - - . - - - - - . . . . F .
9 Offl_
10      Card 25 CMIC Interface Card      Port: 0
11 LoadCd_  MS 0      .
12 QueryCd_ MS 1      . F
13 Card_
14 QueryMS  SHELF:
15 Trnsl_   CARD:
16
17 Next
18 Port_
NAME
Time 14:39 >
    
```

0
.
S

. - in service
S - system busy
T - in test
M - manual busy

10 Determine the action to take:

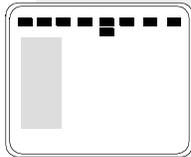
| If | Do |
|---|--|
| the CMIC Interface card state is not in service (.) | Busy and RTS the card. |
| the port state is system busy | Verify that the ATM connections between the MS and the Message Card are intact. Busy and RTS the port. |

| If | Do |
|-------------------------------|--|
| the port state is manual busy | Ensure that no other personnel are performing maintenance on the link and use the RTS command to return the port to service. |
| the port state is in test | Wait for the maintenance activity to complete and then determine the new state. |

11 This procedure is complete.

MC ETH major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      MC      Unit: 0  
               .      .      .      .      ETH
```

Indication

A CCA345 log report is generated when the alarm is raised. A CCA645 log report is generated when the alarm clears.

Meaning

A minor severity alarm indicates that 1 or 2 Ethernet links are down, but that no Message Controller is isolated.

A major severity alarm indicates that a Message Controller is isolated and at least 2 Ethernet links are down.

Action

At the Call Agent Manager

- 1 Enter the MCMtc level.

MCMtc

- 2 Determine the link status.

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        ETH
MCMtc         Blade:   Eth0:    Eth1:    Atm0:    Atm1:
0 Quit        MC0    .      S Inact  . Act    open     open
2             MC1    .      . Inact  . Act    open     open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
   mtc
Time 13:12 >

```

The screenshot shows a terminal window with the following content:

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        ETH
MCMtc         Blade:   Eth0:    Eth1:    Atm0:    Atm1:
0 Quit        MC0    .      S Inact  . Act    open     open
2             MC1    .      . Inact  . Act    open     open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
   mtc
Time 13:12 >

```

A box highlights the link status for Eth0 and Eth1, and an arrow points to a legend box:

```

. - the Ethernet link is available
S - the Ethernet link is down
U - the Ethernet link state is unknown

```

- 3 Determine the next action:

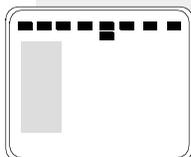
| If | Do |
|--|---|
| one link is down and the alarm is minor | Verify that the cable is installed properly. Verify that the CS LAN router port is configured properly. |
| two links are down and the alarm is minor (one link down on each Message Controller) | No Message Controllers are isolated. Verify that the redundant CS LAN router is in service. Verify that the CS LAN router ports are configured properly. Verify that the cables are installed properly. |

| If | Do |
|---|--|
| two links are down and the alarm is major | Both links are down to a single Message Controller. The Message Controller is isolated. Busy the isolated Message Controller and then lock and unlock the isolated Message Controller from the CS 2000 SAM21 Manager client. |
| the alarm is critical | At least three links are down and at least one of the Message Controllers is isolated. Contact Nortel support personnel. |

4 This procedure is complete.

MC MCTbl major or minor

Alarm display



```
CallAgent      SYS      CON      APPL      MC      Unit: 0  
      .      .      .      .      MCTbl
```

Indication

A CCA344 log report is generated when the alarm is raised. A CCA644 log report is generated when the alarm clears.

Meaning

This alarm is used to report Network Time Protocol (NTP), CPU usage, memory usage, disk usage, and zombie process alarms on the Message Controller.

Action

At the Call Agent Manager

- 1 Enter the MCMtc level.

MCMtc

2 Use the Alarm command to determine the alarm type.

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        MCTbl
              M
MCMtc         Blade:   Eth0:    Eth1:    Atm0:   Atm1:
0 Quit        MC0      .        . Inact  . Act   open   open
2             MC1      .        . Inact  . Act   open   open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10            MC alarms for unit 0: none
11
12            MC alarms for unit 1:
13 LogQuery
14 Alarm      Alarm Severity Description
15 QueryIP    MCTbl  major    MC0: Host is not synchronized to any NTP
16                                     server(s); No. of configured server(s): 2;
17 Help                                     No. of accessible server(s): 1.
18 Refresh
   mtc
Time 14:44 >

```

3 Determine the next action:

| If | Do |
|-----------------------------|---|
| the alarm is related to NTP | Monitor the alarm and wait up to ten minutes to clear. If the alarm doesn't clear, continue to step 4 . |
| otherwise | Proceed to step 4 to reset the Message Controller card. |

- 4 Translate the ATM links from the Message Controller to the Message Switch (MS).

Trns1 <mc_no>

**Example
Trns1 0**

The Message Switch number, card number, and port number are returned. Map the ATM ports to the ms_no, card_no, and port_no on the Message Switch.

```

CallAgent      SYS      CON      APPL      MC      Unit: 0
.              .        .        .        MCTb1
              .        .        .        M
MCMtc         Blade:   Eth0:    Eth1:    Atm0:   Atm1:
0 Quit        MC0     .        . Inact  . Act   open   open
2 Bsy        MC1     .        . Inact  . Act   open   open
3 Rts
4
5 QryLd
6 QryHits
7 ClrHits
8 Trns1
9
10
11             Connectivity report for MC0 retrieved on:
12             Mon Mar 10 13:53:16 2003
13 LogQuery
14 Alarm
15
16
17 Help        ATM0 connected to: 0 24 0   NO   GOOD
18 Refresh    ATM1 connected to: 1 25 0   NO   GOOD
   mtc
Time 13:53 > TRNSL 0

```

At the MAP

5 Enter the MS level.

>MAPCI;MTC;MS

6 Determine the correct MS shelf to use.

| | MS | IOD | Net | PM | CCS | Lns | Trks | Ext | APPL |
|----|------|------|----------------|----|--------|-------|------|---------------|------|
| | . | . | . | . | . | . | . | . | . |
| MS | | | Message Switch | | Clock | Shelf | 0 | Inter-MS Link | 0 1 |
| 0 | Quit | MS 0 | . | | Slave | . | | | .. |
| 2 | | MS 1 | . | | Master | . | | | .. |
| 3 | | | | | | | | | |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | Tst_ | | | | | | | | |
| 7 | Bsy_ | | | | | | | | |

7 Use the Shelf command to enter the Shelf level.

>SHELF <shelf_no>

Example

>SHELF 0

8 Use the information from [step 4](#) to busy the ports to the Message Controller card.

>CARD <card_no>; BSY <ms_no> PORT <port_no>

Example

>CARD 24; BSY 0 PORT 0

>CARD 25; BSY 1 PORT 0 FORCE

Both ATM links to the Message Controller are set to manual busy. Two CMIC alarms, "02CMIC" are raised at the MAP and a

major ATM alarm is raised at the Call Agent Manager. Two MS301 log reports and two CCA340 log reports are generated.

```

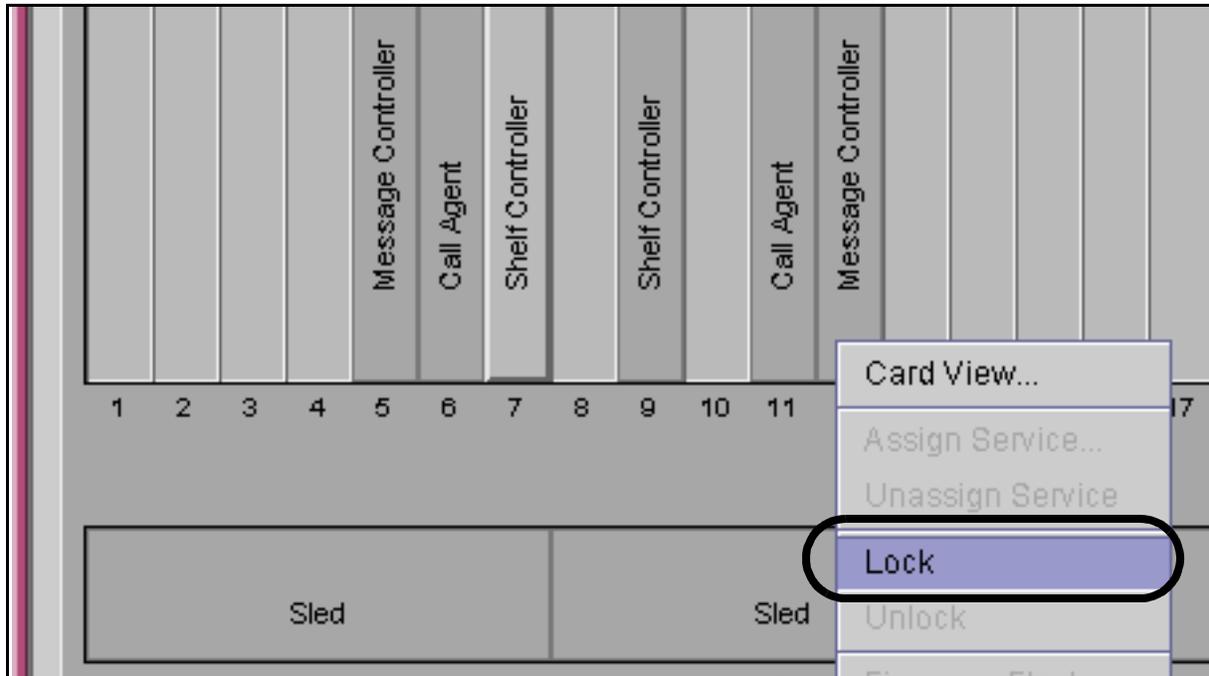
      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
      02CMIC      .      .      .      .      .      .      .      .

MS      Message Switch      Clock      Shelf      0      Inter-MS Link      0      1
0 Quit      MS 0      .      Slave      F      .      .
2      MS 1      .      Master      F      .      .
3
4      Shelf 0      1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
5      Card      1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
6 Tst_      Chain      |      |
7 Bsy_      MS 0      . . . - . . - - - . - - - - - . - - - - - . . F . .
8 RTS_      MS 1      . . . - . . - - - . - - - - - . - - - - - . . . F .
9 Offl_
10      Card 25 CMIC Interface Card      Port: 0
11 LoadCd_      MS 0      .
12 QueryCd_      MS 1      .      M
13 Card_
14 QueryMS      SHELF:
15 Trnsl_      CARD:
16
17 Next
18 Port_
      MIKEM
Time 14:39 >CARD 24; BSY 0 PORT 0; CARD 25; BSY 1 PORT 0 FORCE

```

At the CS 2000 SAM21 Manager client workstation

- 9 From the Shelf View, right click on the card and select Lock from the context menu.

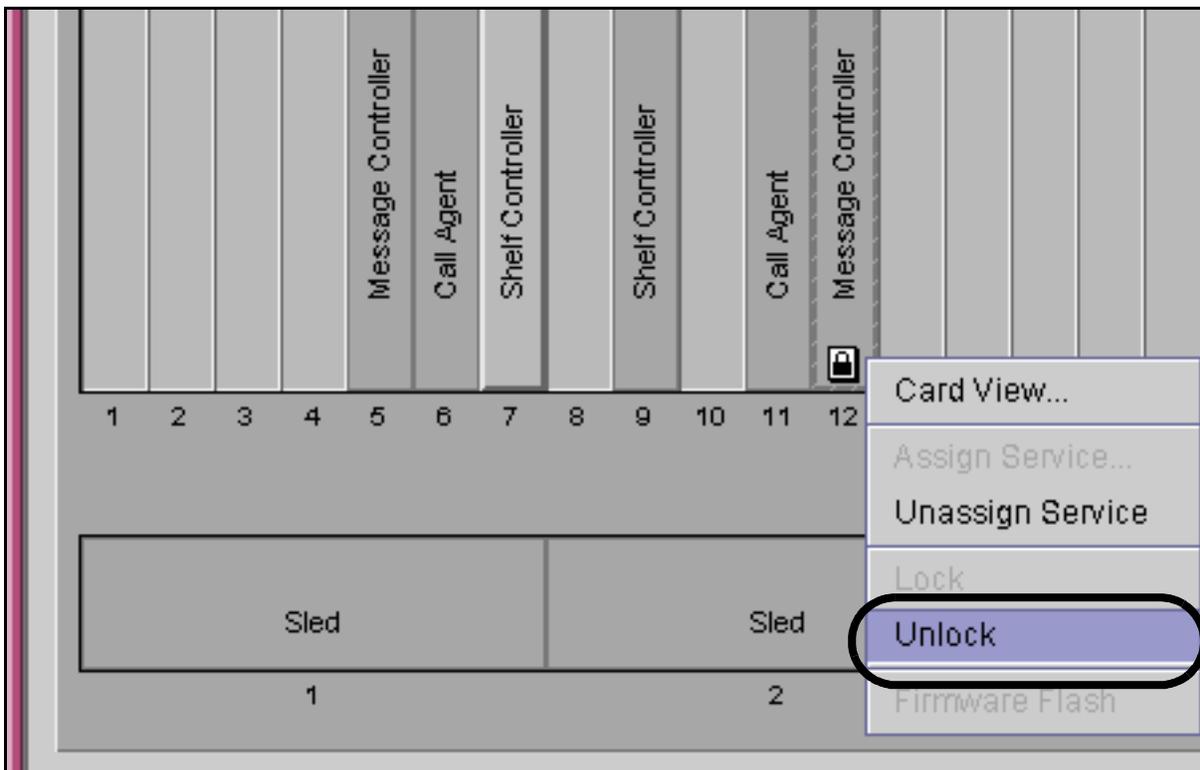


The Message Controller is removed from service. No new alarms are raised at the MAP. The Call Agent Manager reports the card as "blade out-of-service." An SCU500 log report is generated by the SAM21 Shelf Controller to indicate the state change to locked-disabled-none.

- 10 Wait for the lock icon to appear on the selected card.
- 11 Optionally run brief diagnostics on the replacement card. Refer to procedure [Running diagnostics](#).
- 12 Right click on the card icon and select Unlock from the Shelf View. Optionally monitor the download from the States tab of the Card View window.

Wait for the lock icon to disappear from the card on the Shelf View. An SCU500 log report is generated by the SAM21 Shelf Controller to record the state change to unlocked-enabled-none.

At the Call Agent Manager, the Message Controller transitions from offline to in service and the ATM alarm clears. Two CCA640 log reports are generated.



At the MAP

13 Return to service the ports that were busied.

```
>CARD <card_no>; RTS <ms_no> PORT <port_no>
```

Example

```
>CARD 24; RTS 0 PORT 0
```

```
>CARD 25; RTS 1 PORT 1
```

The ports change state from manual busy (M) to in service (.) and the CMIC alarms clear from the MS area of the alarm banner. At the Call Agent Manager, the ATM port transition from

open, to maintenance open, and back to open. Two MS300 log reports are generated.

```

      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
      .      .      .      .      .      .      .      .      .

CARD
0 Quit      MS 0      .      .      .      .      .      .      .
2          MS 1      .      .      .      .      .      .      .
3
4          Shelf 0      .      .      .      .      .      .      .
5          Card 1 2 3 4 5 6 7 8 9 0 1 2 3
6 Tst_      Chain      |      |
7 Bsy_      MS 0      . . . . - . - - . . - .
8 RTS_      MS 1      . . . . - . - - . . - .
9 Offl_
10         Card 04 CMIC Interface Card      Port: 0 1
11 LoadCd_  MS 0      .      .      .      .      .      .
12 QueryCd_ MS 1      .      .      .      .      .      .
13 Card_
14 QueryMS
15 Trnsl_
16
17 Next
18 Port_
  MIKEM
Time 11:39 >RTS 0 PORT 0; RTS 1 PORT 1

```

14 This procedure is complete.