Carrier VoIP

Call Agent Security and Administration

NN10175-611

Document status: Standard
Document version: 07.02
Document date: 20 October 2006

Call Agent Security and Administration

Each of the three interfaces to the Call Agent has security features and user administration.

- Call Agent Manager
- MAP
- CS 2000 SAM21 Manager client

New in this release

Feature changes

See the following sections for information about feature changes.

Gigabit Ethernet interface for sparing for Compact Call Agent cards

This feature is applicable only to the CS2100 for the enterprise market.

In this release, feature A00012478 introduces the Gigabit Ethernet interface for sparing for MCPN905-based Compact Call Agent (CCA) cards. (MCPN765-based CCA cards continue to use fiber channel sparing.) The introduction of Gigabit Ethernet sparing causes the following changes in this document.

- We have added the procedure "Querying the sparing link for CCA cards" (page 83). You can use the procedure to find out whether the fiber channel interface or the Gigabit Ethernet interface is currently selected.
- We have updated some of the illustrations of MAP screens in the document, as follows.
  - — “Sparing link” or “SL” appears where “fiber channel” or “FC” formerly appeared.
  - — Under Compact Call Agent Maintenance (CCAMTC) in the MAP interface, there is a new command to query the sparing link. The command is “16 QuerySL”. You can use the command to find out whether the fiber channel interface or the Gigabit Ethernet interface is selected for sparing.

Security changes associated with feature A00015703

Feature A00015703 gives you the ability to edit the logon banner of a call agent card, and to set passwords to user-defined values. Therefore, we have added the following procedures this document.

- "Editing the logon banner of a call agent card" (page 7)
- "Setting the root password of a call agent card" (page 14)
- "Setting the mtc password of a call agent card" (page 23)

We have also added the procedure "Resetting the root password of a call agent card" (page 21). You will need to use this procedure only if you set the root password and subsequently forget the password.

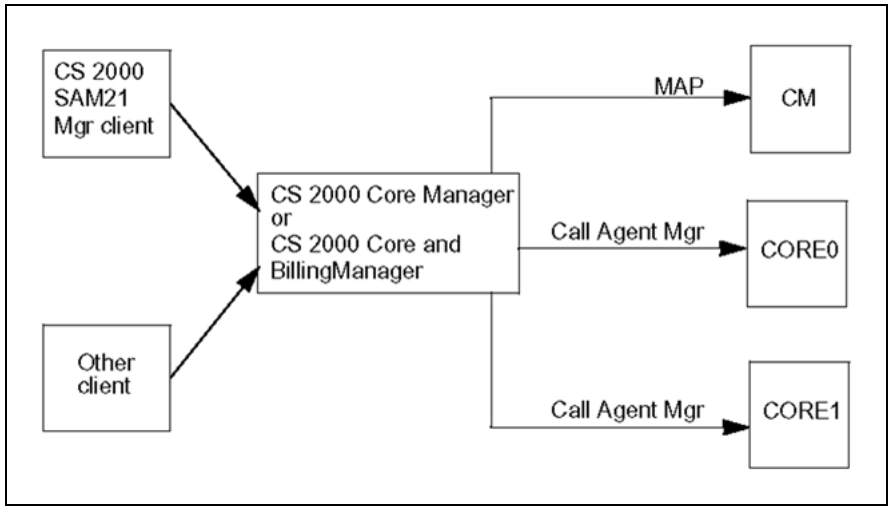
Other changes

There are no other changes in this release.

Security strategy overview

The Call Agent platform hardware and software is protected by the CS 2000 SAM21 Manager server and client. For security features about these elements, refer to the *CS 2000 Management Tools Security and Administration*, NN10172-611.

The Call Agent Manager and MAP are available after the PassThru feature is configured on the CS 2000 Core Manager or Core and Billing Manager (CBM). Logging into the CS 2000 Core Manager with one of the configured PassThru usernames provides a connection between the local machine and the Call Agent Manager or MAP



Access to the MAP is available by telnetting to the CS 2000 Core Manager or Core and Billing Manager (CBM) as user "cmusr" and then logging in with a valid username and password. This username, like the next two,

are Nortel suggested names, but the usernames are configurable when the PassThru feature is configured at the CS 2000 Core Manager or Core and Billing Manager (CBM).

Access to the Call Agent Manager on the unit 0 Call Agent is available by telnetting to the CS 2000 Core Manager or Core and Billing Manager (CBM) as user "core0usr" and then providing a valid username and password. Once logged in, type **ccamtc** and press the Enter key.

Access to the Call Agent Manager on unit 1 Call Agent is available by telnetting to the CS CS 2000 Core Manager or Core and Billing Manager (CBM) as user "core1usr" and then providing a valid username and password. Once logged in, type **ccamtc** and press the Enter key.

User authentication is required at the client workstation, and the destination host.

Call Agent Manager procedures

The Call Agent Manager provides an interface to the platform software and utilities of the Call Agent. Platform software includes the operating system and other non-call processing software.

User administration is available for the Call Agent platform software. Refer to "Changing a user password" (page 59) and "Performing platform user administration" (page 60) for details.

Editing the logon banner of a call agent card

The Call Agent card has a logon banner. The logon banner appears when you log on to the card using an xterm window in the linux operating system.

This module contains two procedures, and you can use either procedure to edit the logon banner of a call agent card.

Interval

Perform this procedure as required.

Prerequisites

The prerequisites are as follows:

- You must have a terminal connected to a computer that enables you to access the call agent card whose logon banner you intend to edit. You can use a Linux terminal, that is, a terminal connected to a computer that is running the Linux operating system, which allows you to create an xterm window. Alternatively, you can use a Windows terminal, that is, a terminal connected to a computer running a Windows operating system. The Windows computer must have third-party ssh software. The Linux computer or Windows computer must be able to access the CS LAN--for example, by way of the 8600 switch.
- You must know the hostname and domain of the server that controls the call agent card whose logon banner you want to edit. The server can be either a Core Billing Manager (CBM) or a SuperNode Data Manager (SDM).
- You must know a username and password that you can use to log on to the CBM or SDM that controls the call agent card whose logon banner you want to edit.
- You must know the root password of the CBM or SDM.
- You must know the IP address of the call agent card whose logon banner you intend to edit.
- You must know the current password of the mtc user of the card, and the current password of the root user of the card.

Common Procedures

This procedure does not refer to any common procedures.

Action

This module contains two procedures, and you can use either procedure to edit the logon banner of a call agent card. The procedures are

- "Editing the logon banner by using the passthru user of the CBM/SDM" (page 8)
- "Editing the logon banner by logging on to the CBM/SDM as root and then telnetting to the call agent" (page 10)

Editing the logon banner by using the passthru user of the CBM/SDM

Step	Action

At the Linux or Windows terminal

1 From the Linux computer or the Windows computer, connect to the CBM or SDM that controls the call agent card. You can log on to the system using the passthru user of CBM/SDM.

If you are using a Linux computer, you type commands in the xterm window. If you are using a Windows computer equipped with third-party ssh software, take the steps necessary to initiate that software, and type commands at the appropriate prompt.

Type

```
ssh hostname.domain -l username
```

and press the Enter key

where

<hostname> is the hostname of the CBM or SDM

<domain> is the domain name of the CBM or SDM

<username> is a valid user name on the CBM or SDM

For example, to log on to the system using the passthru user of CBM/SDM, log on to the call agent card whose logon banner you intend to edit. Type

```
ssh cbm01.domain01 -l core0usr
```

and press the Enter key.

Example system response:

```
Password:
```

2 Type the password and press the Enter key, the passthru user telnets to core0.

Example system response:

```
Last login:  Tue Jun 27 17:29:02 from 47.165.146.73
************
```

```
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
This is a passthru user.
Please type 'Ctrl+p' and Enter for changing your
password.
type 'Enter' or wait for 5 seconds to continue.
Trying 192.168.51.19...
Connected to core0.
Escape character is '^]'.
login:
```

3 Type

mtc

and press the Enter key.

Example system response:

```
Password:
```

4 Type the password of the mtc user, and press the Enter key.

Example system response:

```
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
SYSTEM VERSION: ncgl_cca_image_9.11.2.1
[mtc@192.168.51.19 mtc]$
```

5 Switch users, to become the root user of the call agent card. Type

su -

and press the Enter key.

Example system response:

```
Password:
```

6 Type the password of the root user, and press the Enter key.

Example system response:

```
SYSTEM VERSION: ncgl_cca_image_9.11.2.1
[root@192.168.51.19 root]#
```

7 Edit the logon banner. The logon banner file is a text file named .logon_banner. In the card, the path to the file is /var/log/.logon_banner. You can edit the logon banner with any text editor software in Linux. Alternatively, you can use an ASCII editor

on another computer and upload the edited logon banner to the file /var/log/.logon_banner on the card.

8 Set the logon banner to the newly edited version. At the root user's prompt, type

```
/usr/admin_bin/setbanner.sh
```

and press the Enter key.

Example system response:

```
Stopping xinedit:   [ OK ]
Starting xinedit:   [ OK ]
[root@192.168.51.19 root]#
```

9 Terminate the session. Type

```
exit
```

and press the Enter key.

10 If you are working in an xterm window, click on the "Close" button in the xterm window.

11 You have completed the procedure.

—End—

Editing the logon banner by logging on to the CBM/SDM as root and then telnetting to the call agent

Step	Action

At the Linux or Windows terminal

1 From the Linux computer or the Windows computer, connect to the CBM or SDM that controls the call agent card.

If you are using a Linux computer, you type commands in the xterm window. If you are using a Windows computer equipped with third-party ssh software, take the steps necessary to initiate that software, and type commands at the appropriate prompt.

Type

```
ssh hostname.domain -l username
```

and press the Enter key

where

<hostname> is the hostname of the CBM or SDM

<domain> is the domain name of the CBM or SDM

<username> is a valid user name on the CBM or SDM

For example, type

ssh cbm01.domain01 -l maint

and press the Enter key.

Example system response:

```
Password:
```

2 Type the password and press the Enter key.

Example system response:

```
Last login:  Tue Jun 27 17:29:02 from 47.165.146.73
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
```

3 You have now logged on to the CBM or SDM. Switch users, to become the root user of the CBM or SDM.

Type

su - root

and press the Enter key.

Example system response:

```
Password:
```

4 Type the root password of the CBM or SDM and press the Enter key.

Example system response:

```
Your password will expire in 12 days.
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
```

5 From the CBM or SDM, log on to the call agent card whose logon banner you intend to edit.

Type

telnet <IP-address>

and press the Enter key

where <IP-address> is the IP address of the call agent card

Example system response:

```
Trying 47.168.18.174 .  .  .
```

```
Connected to 47.168.18.174
Escape character is '^j'.
login:
```

6 Type

mtc

and press the Enter key.

Example system response:

```
Password:
```

7 Type the password of the mtc user and press the Enter key.

Example system response:

```
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
SYSTEM VERSION ngcl_image_10.25.1.0
{mtc@47.168.18.174 mtc] $
```

8 Switch users, to become the root user of the call agent card. Type

su -

and press the Enter key.

Example system response:

```
Password:
```

9 Type the password of the root user and press the Enter key.

Example system response:

```
SYSTEM VERSION: ngcl_image_10.25.1.0
[root@47.168.18.174 root]#
```

10 Edit the logon banner. The logon banner file is a text file named .logon_banner. In the card, the path to the file is /var/log/.logon_banner. You can edit the logon banner with any text editor software in Linux. Alternatively, you can use an ASCII editor on another computer and upload the edited logon banner to the file /var/log/.logon_banner on the card.

11 Set the logon banner to the newly edited version. At the root user's prompt, type

/usr/admin_bin/setbanner.sh

and press the Enter key.

Example system response:

```
Stopping xinedit:  [ OK ]
Starting xinedit:  [ OK ]
[root@47.168.18.174 root]#
```

12 Terminate the session. Type

`exit`

and press the Enter key.

13 If you are working in an xterm window, click on the "Close" button in the xterm window.

14 You have completed the procedure.

—End—

Setting the root password of a call agent card

Use the procedure in this module to set the root password of a call agent card.

On each call agent card, the default system-generated root password is li69nux.

The root user can change the root password at any time without restrictions.

ATTENTION

Consequences of unsuccessful login attempts

If, during a session, you make five unsuccessful attempts to log on to cards as root, the system disconnects the session. If you make three consecutive unsuccessful attempts to log on to cards as root, the system disables your account.

Interval

Perform this procedure as required.

Prerequisites

The prerequisites are as follows:

- You must have a terminal connected to a computer that enables you to access the call agent card whose root password you intend to set. You can use a Linux terminal, that is, a terminal connected to a computer that is running the Linux operating system, which allows you to create an xterm window. Alternatively, you can use a Windows terminal, that is, a terminal connected to a computer running a Windows operating system. The Windows computer must have third-party ssh software. The Linux computer or Windows computer must be able to access the CS LAN--for example, by way of the 8600 switch.
- You must know the hostname and domain of the server that controls the call agent card whose root password you want to set. The server can be either a Core Billing Manager (CBM) or a SuperNode Data Manager (SDM).
- You must know a username and password that you can use to log on to the CBM or SDM that controls the call agent card whose root password you want to set.
- You must know the root password of the CBM or SDM.
- You must know the IP address of the call agent card whose root password you want to set.
- You must know the current password of the mtc user of the card, and the current password of the root user of the card.

Common procedures

This procedure does not refer to any common procedures.

Action

Use the following procedure to set the root password of a call agent card.

Setting the root password of a call agent card

Step	Action
1	From the Linux computer or the Windows computer, connect to the CBM or SDM that controls the call agent card. If you are using a Linux computer, type commands in the xterm window. If you are using a Windows computer equipped with third-party ssh software, take the steps necessary to initiate that software, and type commands at the appropriate prompt. Type **`ssh hostname.domain -l username`** and press the Enter key where <hostname> is the hostname of the CBM or SDM <domain> is the domain name of the CBM or SDM <username> is a valid user name on the CBM or SDM For example, type **`ssh cbm01.domain01 -l maint`** and press the Enter key. *Example system response:* `Password:`

2	Type the password and press the Enter key.
	
	Example system response:
	`Last login: Tue Jun 27 17:29:02 from 47.165.146.73`
	`************`
	`This is a private database.`
	`All activity is subject to monitoring.`
	`Any UNAUTHORIZED access or use is PROHIBITED.`
	`************`

3	You have now logged on to the CBM or SDM. Switch users, to become the root user of the CBM or SDM. Type

su - root

and press the Enter key.

Example system response:

```
Password:
```

4 Type the root password of the CBM or SDM and press the Enter key.

Example system response:

```
Your password will expire in 12 days.
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
```

5 From the CBM or SDM, log on to the call agent card whose password you intend to set.

Type

telnet <IP-address>

and press the Enter key

where <IP-address> is the IP address of the call agent card

Example system response:

```
Trying 47.168.18.174 .  .  .
Connected to 47.168.18.174
Escape character is '^j'.
login:
```

6 Type

mtc

and press the Enter key.

Example system response:

```
Password:
```

7 Type the password of the mtc user, and press the Enter key.

Example system response:

```
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
SYSTEM VERSION ngcl_image_10.25.1.0
{mtc@47.168.18.174 mtc] $
```

8 Switch users, to become the root user of the call agent card. Type

su -

and press the Enter key.

Example system response:

```
Password:
```

9 Type the password of the root user and press the Enter key.

Example system response, indicating no errors:

```
SYSTEM VERSION: ngcl_image_10.25.1.0
[root@47.168.18.174 root]#
```

Example system response, indicating a synchronization error:

```
testing time synchronization in nfs server
/usr/sbin/nfstimetest:  time on /var/log is not synced
with core, manual action required
unable to complete command, sync time on NFS first
```

10 Select the next step as follows:

If	Do
the system response to step 9 indicated a synchronization error	step 11
the system response to step 9 did not indicate an error	step 17

11 Type

ntpupdate -u <IP-address>

where

<IP-address> is the IP address of the network time protocol (NTP) server

For example, type

ntpupdate -u 47.111.11.1

and press the Enter key.

Example system response:

```
11 Oct 16:21:07 ntpupdate[1868]:  adjust time server
47.111.11.1 offset - 0.000208 sec
```

Leave the call-agent session running. Do not log out nor terminate the call-agent session. You will resume working in the call-agent session when you reach step 17.

12 Go to a different terminal and initiate a session on the STORM. Type

ssh root@<IP-address>

where

<IP-address> is the IP address of the STORM

For example, type

ssh root@47.168.39.112

and press the Enter key.

Example system response:

```
password:
```

13 Type the password of the root user of the STORM and press the Enter key.

Example system response:

```
Last login:  Thu Oct 12 11:15:57 2006 from 47.165.145
.29
[root@TPCSTORM root]#
```

14 Type

ntpupdate -u <IP-address>

where

<IP-address> is the IP address of the network time protocol (NTP) server

For example, type

ntpupdate -u 47.111.11.1

and press the Enter key.

Example system response:

```
Looking for host 47.111.11.1 and service ntp
host found:  47.111.11.1
11 Oct 16:23:37 ntpupdate[23040]:  step time server
47.111.11.1 offset - 0.795215 sec
```

15 Terminate the STORM session. Type

logout

and press the Enter key.

Example system response:

```
Connection to TPCSTORM closed.
```

16 Return to the terminal on which the call-agent session is running, and continue to step 17.

17 Indicate that you want to set a new password. Type

passwd

and press the Enter key.

Example system response:

```
testing time synchronization on nfs servers
syncing password files before attempting operation
New UNIX password:
```

18 Type the new root password and press the Enter key.

Example system response:

```
Retype new UNIX password:
```

19 Retype the new root password and press the Enter key.

Example system response:

```
updating backup password files
[root@47.168.18.174 root]#
```

20 Terminate the session. Type

`exit`

and press the Enter key.

21 If you are working in an xterm window, click on the "Close" button in the xterm window.

22 You have completed the procedure.

—End—

Resetting the root password of a call agent card

Use this procedure to reset the root password of a call agent card to the default value. The default root password is li69nux.

If the user-specified root password of a call agent card has been forgotten, then you use this procedure to reset the root password to the default value. Subsequently you should specify a new root password of your choosing.

Note that this procedure resets all user-specified root passwords for all call agent cards in the CS 2000 Compact. Therefore, you must subsequently specify new root passwords for all call agent cards in the CS 2000 - Compact.

Interval

Perform this procedure as required.

Prerequisites

The prerequisites are as follows:

- You must have a terminal connected to a computer that enables you to access the NFS server (STORM). You can use a Linux terminal, that is, a terminal connected to a computer that is running the Linux operating system, which allows you to create an xterm window. Alternatively, you can use a Windows terminal, that is, a terminal connected to a computer running a Windows operating system. The Windows computer must have third-party ssh software. The Linux computer or Windows computer must be able to access the CS LAN--for example, by way of the 8600 switch.
- You must know the IP address of the NFS server (STORM).
- You must know the password of the root user of the NFS server.

Common procedures

This procedure refers to the following other procedures:

- "Locking the Call Agent" (page 77)
- "Unlocking the Call Agent" (page 79)

Action

Use the following procedure to reset the root password of a call agent card to the default value.

Resetting the root password of a call agent card

Step	Action

At the SAM21 Element Manager terminal

1 Perform the procedure "Locking the Call Agent" (page 77). Then continue to the next step in this procedure.

At the Linux or Windows terminal

2 From the Linux computer or the Windows computer, connect to the NFS server (STORM).

If you are using a Linux computer, you type commands in the xterm window. If you are using a Windows computer equipped with third-party ssh software, take the steps necessary to initiate that software, and type commands at the appropriate prompt.

Type

```
ssh root@<IP-address>
```

and press the Enter key

where

<IP-address> is the IP address of the NFS server

For example, type

```
ssh root@47.168.40.113
```

and press the Enter key.

Example system response:

```
Password:
```

3 Type the root password of the NFS server and press the Enter key.

Example system response:

```
STORM-storm-1>
```

4 Delete the following files:

- /nfsserv/3pc/mtc/log1/shadow6
- /nfsserv/3pc/mtc/log1/passwd6
- /nfsserv/3pc/mtc/log1/faillog
- /nfsserv/3pc/mtc/log0/shadow6
- /nfsserv/3pc/mtc/log0/passwd6
- /nfsserv/3pc/mtc/log0/faillog

Note that when you delete these files, you delete all user-specified passwords for all call agent cards in the CS 2000 - Compact.

5 Terminate the session. Type

```
exit
```

and press the Enter key.

6 If you are working in an xterm window, click on the "Close" button in the xterm window.

At the SAM21 Element Manager terminal

7 Perform the procedure "Unlocking the Call Agent" (page 79). Then continue to the next step in this procedure.

8 You have completed the procedure.

—End—

The call agent cards reboot when you unlock them. After they have rebooted, you can log on to each one using the default passwords.

- For the mtc user, the default password is mtc.
- For the root user, the default password is li69nux.

Setting the mtc password of a call agent card

This module contains two procedures, and you can use either procedure to set the mtc password of a call agent card.

On each call agent card, the default system-generated mtc password is mtc.

For a call agent card, the default password for the mtc user is not expected to work any more after the first login. The system should prompt for a new password when the old one expires, and this may happen on the first boot, the first login. For the first boot at least, the user must log on to the system and change the passwords. The user must log on by using the passthru user of CBM/SDM, or by logging on to CBM/SDM as root and then opening a telnet to CCA. Note that the NFS server must be up and running for changes to take effect.

SSH will not accept default users with expired or default passwords. The system is expected to let no one in on first boot. It could open for SSH login with the changed password.

Rules for passwords

Certain limitations have been put on passwords:

- Password reuse limit should be 11.
- A password must be at least six characters long.
- After six or more unsuccessful SSH login attempts, the session should be disconnected (three for telnet via trusted hosts).
- After six consecutive unsuccessful SSH login attempts, the account should be disabled (four for telnet via trusted hosts).

Interval

Perform this procedure as required.

Prerequisites

The prerequisites are as follows:

- You must have a terminal connected to a computer that enables you to access the call agent card whose mtc password you intend to set. You can use a Linux terminal, that is, a terminal connected to a computer that is running the Linux operating system, which allows you to create an xterm window. Alternatively, you can use a Windows terminal, that is, a terminal connected to a computer running a Windows operating system. The Windows computer must have third-party ssh software. The Linux

computer or Windows computer must be able to access the CS LAN--for example, by way of the 8600 switch.

- You must know the hostname and domain of the server that controls the call agent card whose mtc password you want to set. The server can be either a Core Billing Manager (CBM) or a SuperNode Data Manager (SDM).
- You must know a username and password that you can use to log on to the CBM or SDM that controls the call agent card whose mtc password you want to set.
- You must know the root password of the CBM or SDM.
- You must know the IP address of the call agent card whose mtc password you want to set.
- You must know the current password of the mtc user of the card, and the current password of the root user of the card.

Common procedures

This procedure does not refer to any common procedures.

Action

This module contains two procedures, and you can use either procedure to set the mtc password of a call agent card. The procedures are

- "Setting the mtc password by using the passthru user of the CBM/SDM" (page 24)
- "Setting the mtc password by logging on to the CBM/SDM as root and then telnetting to the call agent" (page 27)

Setting the mtc password by using the passthru user of the CBM/SDM

Step	Action

At the Linux or Windows terminal

1 From the Linux computer or the Windows computer, connect to the CBM or SDM that controls the call agent card. For the first boot at least, the user must log on to the system and change the passwords. The user must log on by using the passthru user of CBM/SDM, or by logging on to CBM/SDM as root and then opening a telnet to CCA.

If you are using a Linux computer, type commands in the xterm window. If you are using a Windows computer equipped with third-party ssh software, take the steps necessary to initiate that software, and type commands at the appropriate prompt.

Type

```
ssh hostname.domain -l username
```

and press the Enter key

where

<hostname> is the hostname of the CBM or SDM

<domain> is the domain name of the CBM or SDM

<username> is a valid user name on the CBM or SDM

For example, to log on to the system after the first boot using the passthru user of CBM/SDM to the call agent card whose password you intend to set, type

telnet cbm01.domain01

and press the Enter key.

Example system response:

```
Trying 192.168.51.137...
connected to 192.168.51.137.  Escape character is
'^]^'.
Authorized use only, activities logged.
login:
```

2 Type

core0usr

and press the Enter key.

Example system response:

```
Choose a new password.
New Password:
```

3 Type the new password of the core0usr user and press the Enter key.

Example system response:

```
Re-enter new Password:
```

4 Retype the new password of the core0usr user and press the Enter key.

Example system response:

```
telnet: password successfully changed for core0usr
Last login: Tue Oct 10 15:10:43 from 202.38.46.203
This is a passthru user.
Please type 'Ctrl+p' and Enter for changing
your password.
        type 'Enter' or wait for 5 seconds to continue.

Trying 192.168.51.19...
Connected to core0.
Escape character is '^]'.
Welcome to CCA blade 905
```

```
login:
```

5 Type

`mtc`

and press the Enter key.

Example system response:

```
Password:
```

6 Type the default password of the mtc user and press the Enter key.

Example system response:

```
You are required to change your password immediately
(root enforced)
Changing password for mtc
(current) UNIX password:
```

7 Type the current default password of the mtc user and press the Enter key.

Example system response:

```
New UNIX password:
```

8 Choose a new password that conforms to the rules for passwords. (The rules are listed in the section "Rules for passwords" (page 23).) Type the new password of the mtc user and press the Enter key.

Example system response:

```
Retype new UNIX password:
```

9 Retype the new password of the mtc user and press the Enter key.

Example system response:

```
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
SYSTEM VERSION: ncgl_cca_image_9.11.2.1
[mtc@192.168.51.19 mtc]$
```

10 Terminate the session. Type

`exit`

and press the Enter key.

11 If you are working in an xterm window, click on the "Close" button in the xterm window.

12 You have completed the procedure.

—End—

Setting the mtc password by logging on to the CBM/SDM as root and then telnetting to the call agent

Step	Action

At the Linux or Windows terminal

1 From the Linux computer or the Windows computer, connect to the CBM or SDM that controls the call agent card.

If you are using a Linux computer, type commands in the xterm window. If you are using a Windows computer equipped with third-party ssh software, take the steps necessary to initiate that software, and type commands at the appropriate prompt.

Type

```
ssh hostname.domain -l username
```

and press the Enter key

where

<hostname> is the hostname of the CBM or SDM

<domain> is the domain name of the CBM or SDM

<username> is a valid user name on the CBM or SDM

For example, type

```
ssh cbm01.domain01 -l maint
```

and press the Enter key.

Example system response:

```
Password:
```

2 Type the password and press the Enter key.

Example system response:

```
Last login:  Tue Jun 27 17:29:02 from 47.165.146.73
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
```

3 You have now logged on to the CBM or SDM. Switch users, to become the root user of the CBM or SDM.

Type

su - root

and press the Enter key.

Example system response:

```
Password:
```

4 Type the root password of the CBM or SDM and press the Enter key.

Example system response:

```
Your password will expire in 12 days.
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
```

5 From the CBM or SDM, log on to the call agent card whose mtc password you intend to set.

Type

telnet <IP-address>

and press the Enter key

where <IP-address> is the IP address of the call agent card

For example, type

telnet 192.168.51.137

and press the Enter key.

Example system response:

```
Trying 192.168.51.137...
connected to 192.168.51.137.
Escape character is '^]^'.

Authorized use only, activities logged.
login:
```

6 Type

maint

and press the Enter key.

Example system response:

```
Password:
```

7 Type the password of the maint user and press the Enter key.

Example system response:

```
Your password will expire in 36 days.
Last login:  Wed Oct 11 16:20:00 from 202.38.46.203
```

```
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
cs2k6cbm:Rsh>
```

8 You have now logged on to the CBM or SDM. Switch users, to become the root user of the CBM or SDM. Type

`su - root`

and press the Enter key.

Example system response:

```
Password:
```

9 Type the root password of the CBM or SDM and press the Enter key.

Example system response:

```
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
cs2k6cbm#
```

10 From the CBM or SDM, log on to the call agent card whose mtc password you intend to set. Type

`telnet <IP-address>`

and press the Enter key.

where

<IP-address> is the IP address of the call agent card

Example system response:

```
Trying 192.168.51.19...
Connected to core0.
Escape character is '^]'.
login:
```

11 Type

`mtc`

and press the Enter key.

Example system response:

```
Password:
```

12 Type the default password of the mtc user and press the Enter key.

Example system response:

```
You are required to change your password immediately
(root enforced)
Changing password for mtc
(current) UNIX password:
```

13 Type the current default password of the mtc user and press the Enter key.

Example system response:

```
New UNIX password:
```

14 Choose a new password that conforms to the rules for passwords. (The rules are listed in the section "Rules for passwords" (page 23).) Type the new password of the mtc user and press the Enter key.

Example system response:

```
Retype new UNIX password:
```

15 Retype the new password of the mtc user and press the Enter key.

Example system response:

```
************
This is a private database.
All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED.
************
SYSTEM VERSION: ncgl_cca_image_9.11.2.1
[mtc@192.168.51.19 mtc]$
```

16 Terminate the session. Type

`exit`

and press the Enter key.

17 If you are working in an xterm window, click on the "Close" button in the xterm window.

18 You have completed the procedure.

—End—

Dropping call processing application synchronization

The **DpSync** command is available from the active Call Agent only.

Dropping call processing application synchronization

Step	Action

At the active Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the Appl level.

```
Appl
```

3 Enter the DpSync command.

```
DpSync
```

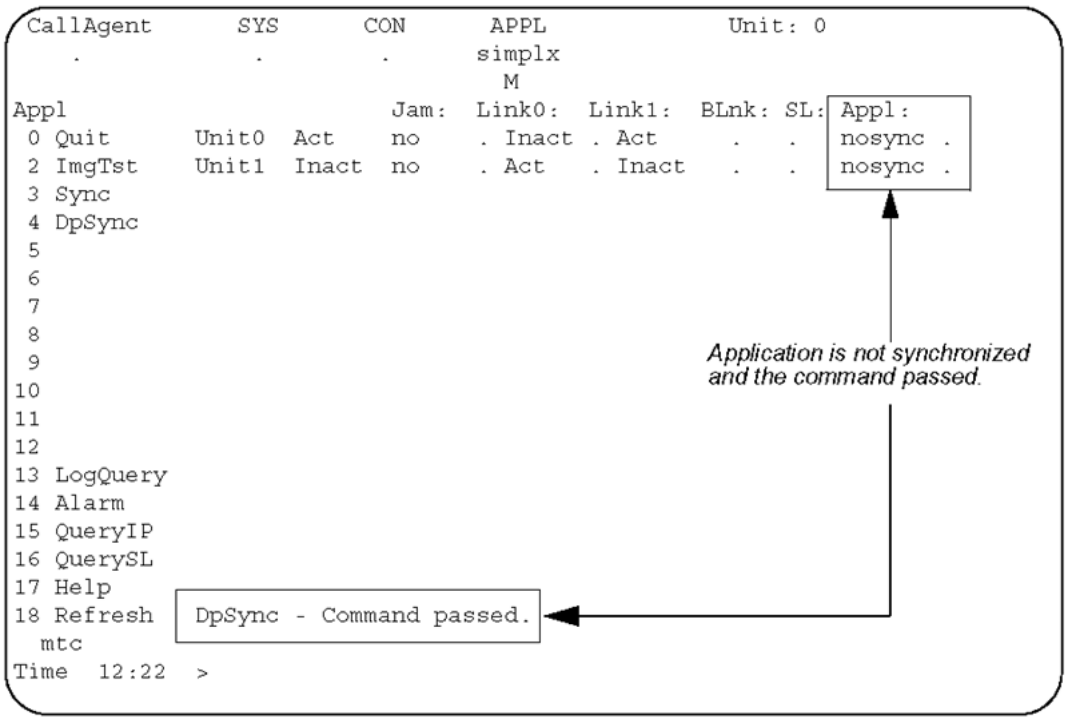
```
CallAgent       SYS       CON       APPL              Unit: 0
    .             .         .      simplx
                                      M
Appl                          Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Act     no     . Inact . Act      .    .   nosync .
 2 ImgTst     Unit1  Inact   no     . Act   . Inact    .    .   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 QuerySL              Parms: [RestartType]
17 Help                    Restart    - ( WARM | COLD | RELOAD | NORESTART )
18 Refresh                 (default) -  COLD
  mtc
Time  12:25
```

4 This procedure is complete.

—End—

Additional information

Successful completion of the command is indicated with a screen similar to the following:



If the command is attempted from the inactive unit, the Call Agent responds:

```
DpSync - Command rejected.  Reason:  Not active unit.
```

Testing application images

The **ImgTst** command is available from the active Call Agent only.

Testing application images

Step	Action

At the active Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the Appl level.

```
Appl
```

3 Enter the ImgTst command.

```
ImgTst
```

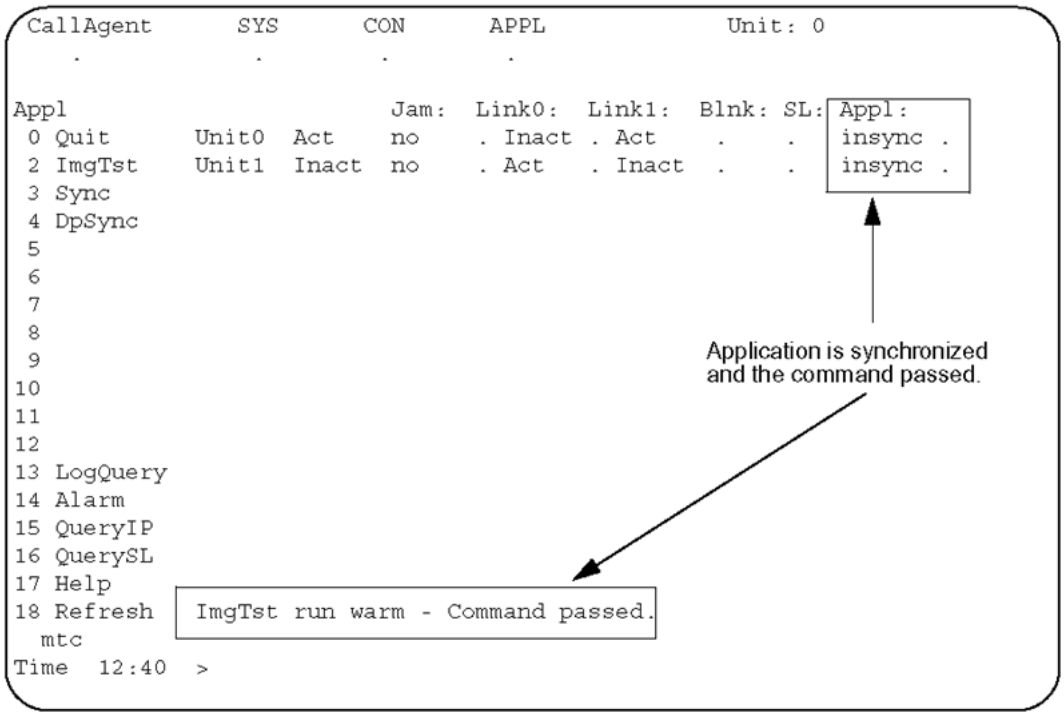
```
CallAgent       SYS       CON       APPL              Unit: 0
    .             .         .      ImgTst

Appl                        Jam:  Link0:  Link1:  Blnk: SL: Appl:
 0 Quit       Unit0  Act    no    . Inact . Act     .    .   nosync .
 2 ImgTst     Unit1  Inact  no    . Act   . Inact   .    .   nosync /imgtst
 3 Sync
 4 DpSync
 5
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm      ImgTst:   Test for image restartability on inactive unit.
15 QueryIP              Parms: RequestType TestType [NOSYNC]
16 QuerySL                 ReqType    - ( RUN | QUERY )
17 Help                    TestType   - ( WARM | COLD | RELOAD )
18 Refresh                 NOSYNC     - for no application sync after test
  mtc
Time  12:30  >imgtst run warm
```

4 This procedure is complete.

—End—

Additional information

Successful completion of the command is indicated with a screen similar to the following:



If the command is attempted from the inactive unit, the Call Agent responds:

```
ImgTst run warm - Command rejected.  Reason:  Not active
unit.
```

Synchronizing call processing applications

The **Sync** command is available from the active Call Agent only.

Synchronizing call processing applications

Step	Action

At the active Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the Appl level.

```
Appl
```

3 Enter the Sync command.

```
Sync
```

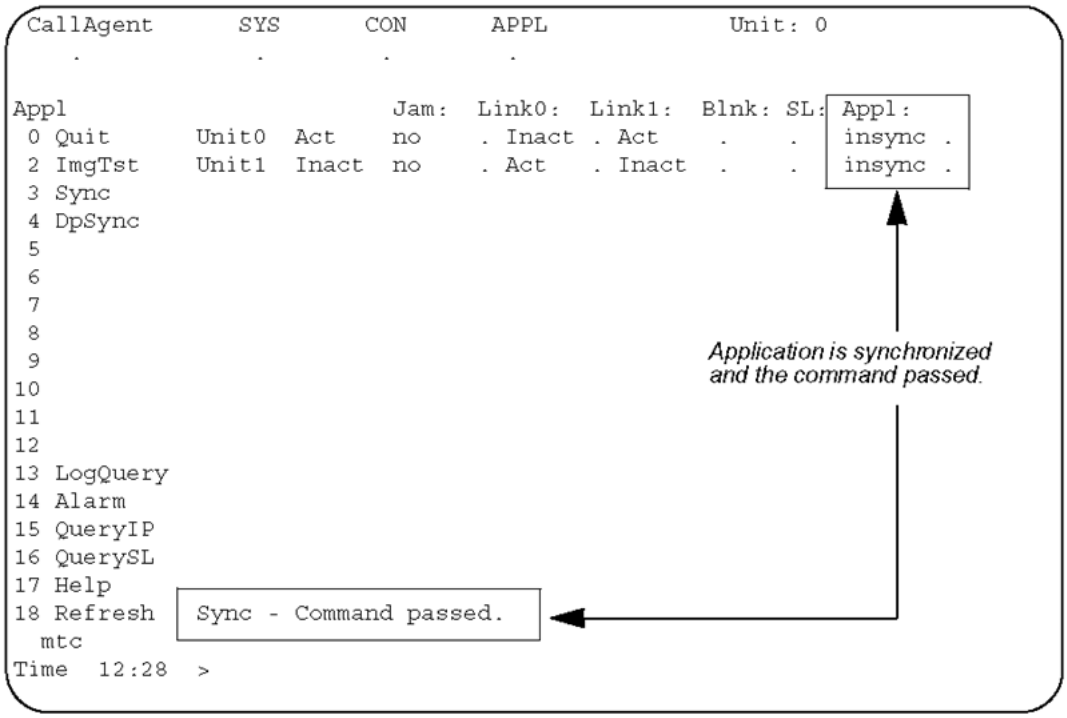
```
 CallAgent       SYS       CON       APPL              Unit: 0
    .              .         .       simplx
                                       M
Appl                          Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Act     no     . Inact . Act     .    .   nosync /syncing
 2 ImgTst     Unit1  Inact   no     . Act   . Inact   .    .   nosync /syncing
 3 Sync
 4 DpSync
 5
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh    Sync:     Synchronize the applications.
  mtc
Time  12:27   >
```

4 This procedure is complete.

—End—

Additional information

Successful completion of the command is indicated with a screen similar to the following:



If the command is attempted from the inactive unit, the Call Agent responds:

```
Sync - Command rejected.  Reason:  Not active unit.
```

Jamming a Call Agent

Jamming the Call Agent places the inactive unit in a maintenance state and prevents a Switch of Activity (SWACT) from the active unit to the inactive unit.

Jamming a Call Agent

Step	Action

At the active Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the CAMtc level.

```
CAMtc
```

3 Enter the Jam command.

```
Jam
```

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

CAMtc                      Jam:  Link0:  Link1:  Blnk: SL: Appl:
 0 Quit       Unit0  Act    no    . Inact . Act     .     .   insync .
 2 Jam        Unit1  Inact  yes   . Inact . Act     .     .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL   Jam:      Jam the inactive unit, to prevent it taking activity.
17 Help                 Parms: [FORCE]
18 Refresh                 FORCE      - bypass system stability checks
  mtc
Time  10:38  >
```

4 This procedure is complete.

—End—

Additional information

The Jam command must be issued from the active Call Agent. A request on the inactive Call Agent is refused with the following message.

```
Jam - Command rejected.  Reason:  Not active unit.
```

Successful execution returns a screen similar to the following figure:

```
CallAgent       SYS       CON       APPL              Unit: 1
  JInact          .         .         .

CAMtc                       Jam:  Link0:  Link1:  Blnk: SL: Appl:
 0 Quit       Unit0  Inact  yes    . Act    . Inact  .     .   insync .
 2 Jam        Unit1  Act    no     . Act    . Inact  .     .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh    Jam - Command passed.
  mtc
Time  12:15  >
```

Releasing a jammed Call Agent

Releasing a jammed Call Agent removes the inactive unit from a maintenance state and prepares the inactive unit for service.

Releasing a jammed Call Agent

Step	Action

At the active Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the CAMtc level.

```
CAMtc
```

3 Enter the RelJam command.

```
RelJam
```

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

CAMtc                       Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Act    no     . Inact . Act     .    .   insync .
 2 Jam        Unit1  Inact  yes    . Inact . Act     .    .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh    RelJam:   Release jam on the inactive unit.
  mtc
Time  10:38  >
```

4 This procedure is complete.

—End—

Additional information

Successful completion returns the following message:

```
RelJam - Command passed.
```

If the command is attempted from the inactive unit, the Call Agent responds:

```
RelJam - Command rejected.  Reason:  Not active unit.
```

Executing a routine exercise test

Routine Exercise Tests (RExTst) are executed every 24 hours as a part of automatic maintenance. Use this procedure to invoke a manual RExTst.

Executing a routine exercise test

Step	Action

At the active Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the CAMtc level.

```
CAMtc
```

3 Enter the RexTst command.

```
RExTst RUN
```

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

CAMtc                      Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Act    no    . Inact . Act     .    .   insync .
 2 Jam        Unit1  Inact  no    . Inact . Act     .    .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP    WARNING: The RExTst command runs an image test, hardware
16 QuerySL             diagnostics, a hardware reset and a reboot of the
17 Help                inactive unit.
18 Refresh    Please confirm ("YES", "Y", "NO", or "N"):
  mtc
Time  14:07   >
```

4 Confirm the test.

System response:

The system runs the REx test, and initiates a controlled hot SwAct. For more information on the controlled hot SwAct, refer to Changing REx Tst (routine exercise test) intensity in this document.

5 Query the results of the RexTst.

```
RExTst QUERY
```

6 This procedure is complete.

—End—

Additional information

The command must be run from the active unit or the system rejects the command with the following message:

```
RExTst run - Command rejected.  Reason:  Not active unit.
```

Progress indicators

During the routine exercise test, the screen looks similar to the following figure:

```
CallAgent       SYS       CON       APPL              Unit: 1
  RExTst          .         .       ImgTst

CAMtc                       Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Inact  no    . Act   . Inact  .     .   nosync /imgtst
 2 Jam        Unit1  Act    no    . Act   . Inact  .     .   nosync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP    WARNING: The RExTst command runs an image test, hardware
16 QuerySL             diagnostics, a hardware reset and a reboot of the
17 Help                inactive unit.
18 Refresh    Please confirm ("YES", "Y", "NO", or "N"):
  mtc
Time  14:08   >y
```

Queried results for success routine exercise tests look similar to the following figure.

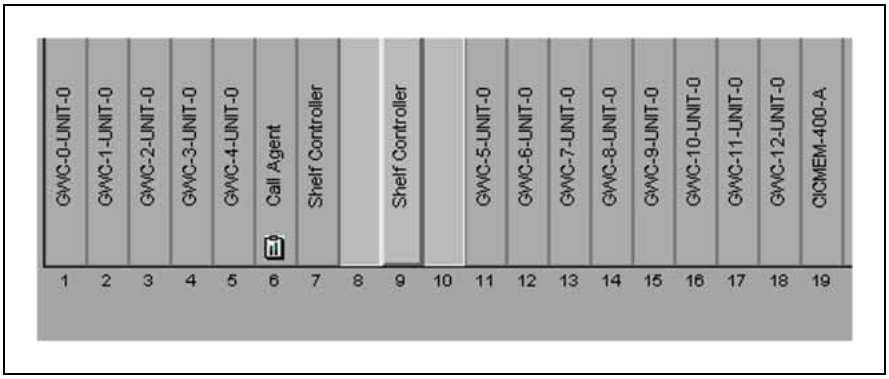
```
CallAgent       SYS       CON       APPL              Unit: 1
    .             .         .         .

CAMtc                       Jam:  Link0:  Link1:  BLnk: SL: Appl:
 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
12            Results for QUERY LAST REX TEST:
13 LogQuery
14 Alarm       Last run on: Mon Nov  5 12:32:03 2001
15 QueryIP     Unit Tested: 0
16 QuerySL       Initiator: MANUAL
17 Help              Class: FULL
18 Refresh          Result: PASSED
  mtc
Time  12:36  >
```

CS 2000 SAM21 Manager client progress indicators

The RExTst has four stages:

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

During stages 2 and 3, the CS 2000 SAM21 Manager client indicates that the Call Agent is unlocked-disabled-in test. Otherwise, the Call Agent appears as unlocked-enabled-none. The following figure shows the Call Agent in the unlocked-disabled-intest state.



After the RExTst completes successfully, the Call Agent is restored to unlocked-enabled-none. If the RExTst fails, the Call Agent card icon turns red and the SAM21 Shelf Controller begins recovery of the Call Agent.

Log reports

Successful completion of the RExTst generates the following logs:

- CCA660 "REx Test Started"
- CCA620 "Image Test Started"
- CCA315 "Application Out-of-Sync (simplex)"
- CCA616 "Application In-Service"
- CCA615 "Application In-Sync"
- CCA621 "Image Test Finished"
- CCA661 "REx Test Finished"

Use the **`LogQuery`** command from the Call Agent Manager to review logs.

Canceling a routine exercise test

This procedure requires a second log in to the active Call Agent card.

Canceling a routine exercise test (RExTst) is only available during the image test (ImgTst) and synchronization (sync) stages of the RExTst. The command is rejected during the diagnostics stage of the RExTst and when the Call Agent is rebooting.

Canceling a routine exercise test

Step	Action

At the active Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the CAMtc level.

```
CAMtc
```

3 Terminate the RExTst.

```
RExTst TERMINATE
```

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

CAMtc                       Jam:  Link0:  Link1:  Blnk: SL: Appl:
 0 Quit       Unit0  Act    no    . Inact . Act     .     .   insync .
 2 Jam        Unit1  Inact  no    . Inact . Act     .     .   insync .
 3 RelJam
 4 RExTst
 5 SwAct
 6
 7
 8
 9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh
  mtc
Time  07:57  >
```

4 This procedure is complete.

—End—

Performing a maintenance switch of activity on a Call Agent

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

Performing a maintenance switch of activity on a Call Agent

Step	Action

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
    .            .         .       simplx
                                      M
Appl                          Jam:  Link0:  Link1:  Ser: SL: Appl:
 0 Quit       Unit0  Act     no     . Inact . Act     .   NA  nosync .
 2 ImgTst     Unit1  Inact   no     . 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 QuerySL              Parms: [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.
```

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 proceding with NORESTARTSWACT.

6 Check status:

```
> BCSUPDATE;SWACTCI;STATUSCHECK
```

Success is indicated as follows:

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

7 Execute the NORESTARTSWACT:

```
> NORESTARTSWACT
```

ATTENTION

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).

ATTENTION

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 an N.

14 You have completed this procedure.

—End—

Retrieving IP addresses

Retrieving IP addresses

Step	Action

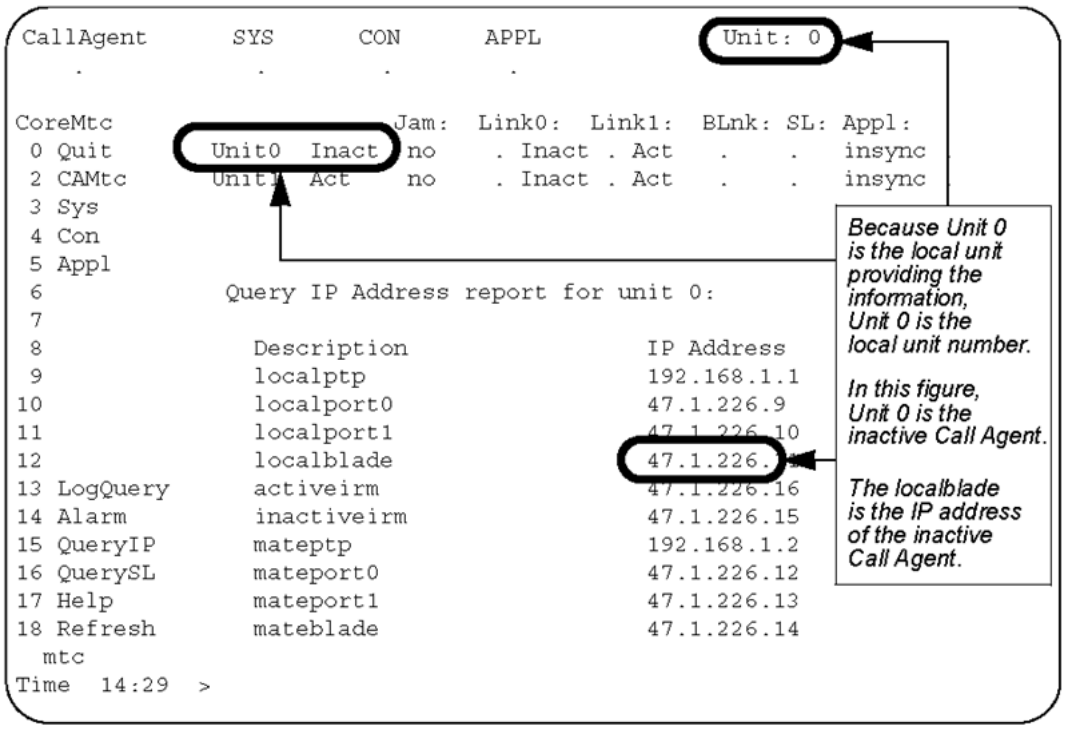
At the Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the QueryIP command.

```
QueryIP
```



3 This procedure is complete.

—End—

Additional information

The IP address scheme is as follows:

- localptp and mateptp

These addresses are Point to Point (PTP) links from one unit to the other. This link is created on the sparing link interface (fiber channel or Gigabit Ethernet) and is used for maintenance messaging. It is not available to users.

Note that the feature supporting the use of the Gigabit Ethernet interface is applicable only to the CS2100 for the enterprise market.

- localport0, localport1, mateport0, and mateport1

  These addresses reflect the first and second 100BaseT Ethernet interfaces for each unit.

- localblade and mateblade

  These are virtual addresses that are mapped to the active ethernet port on each unit.

- activeirm and inactiveirm

  These are virtual addresses. The address of the activeirm is the address of the call processing application.

The IP addresses for localblade and mateblade are provisioned by Nortel Installation Services Technology personnel at the CS 2000 SAM21 Manager client. Software calculates the rest of the IP addresses from the localblade and mateblade addresses. These other IP addresses are not provisionable.

Busying an Ethernet link

Busying an Ethernet link

Step	Action

At the Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the Con level.

```
Con
```

3 Enter the BsyLnk command.

```
BsyLnk
```

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

Con                          Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Inact   no     . Act    . Inact  .     .   insync .
 2            Unit1  Act     no     . Act    . Inact  .     .   insync .
 3
 4
 5
 6
 7 BsyLnk
 8 RTSLnk
 9 SwLnk
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL    BsyLnk:   Manually take a link out of service.
17 Help                 Parms: LinkNumber
18 Refresh                 LinkNum    -  0 or 1
  mtc
Time  09:13  >
```

The state changes from in-service (.) to manual busy (M)

4 This procedure is complete.

—End—

Additional information

The BsyLnk command must be issued on the inactive link. The command is rejected on the active link with the following message.

```
BsyLnk 1 - Command rejected.  Reason:  cannot lock active
link.
```

Successful completion of the command is indicated with a message similar to the following.

```
BsyLnk 0 - Command passed.
```

Returning to service an Ethernet link

Returning to service an Ethernet link

Step	Action

At the Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the Con level.

```
Con
```

3 Enter the RTSLnk command.

```
RTSLnk
```

```
CallAgent       SYS       CON       APPL              Unit: 0
    .             .     LnkCon       .
                          M
Con                        Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Inact  no    . Act   M Inact  .    .   insync .
 2            Unit1  Act    no    . Act   . Inact  .    .   insync .
 3
 4
 5
 6
 7 BsyLnk
 8 RTSLnk
 9 SwLnk
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL    RTSLnk:   Manually return to service a link.
17 Help                 Parms: LinkNumber
18 Refresh                 LinkNum    -  0 or 1
  mtc
Time  09:14  >
```

4 This procedure is complete.

—End—

Additional information

The RTSLnk command must be issued on a busied link. The command is rejected on an unlocked link with the following message.

```
RTSLnk 1 - Command rejected.  Reason:  link already unlocked.
```

Successful completion of the command is indicated with a message similar to the following.

```
RTSLnk 0 - Command passed.
```

This command also clears a major connection alarm that is caused by a manually busied 100BaseT Ethernet link.

Switching Ethernet link activity

Switching Ethernet link activity

Step	Action

At the Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the Con level.

```
Con
```

3 Enter the SwLnk command.

```
SwLnk
```

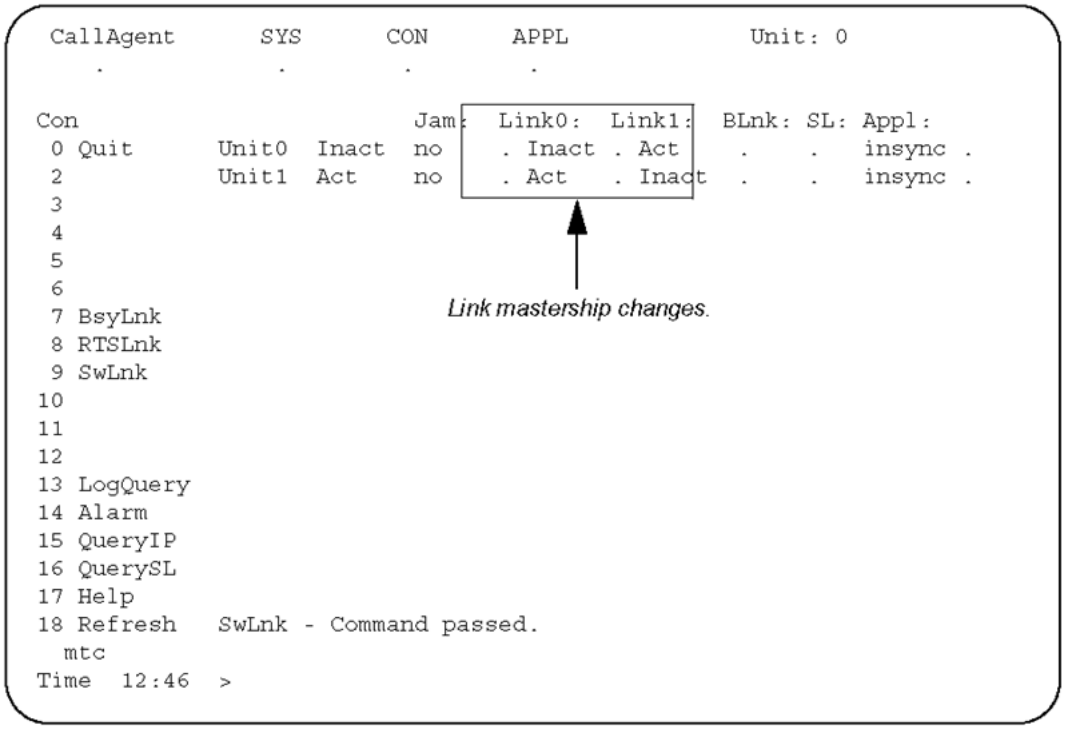
```
 CallAgent       SYS       CON       APPL              Unit: 0
    .             .         .         .

Con                        Jam:  Link0:  Link1:  BLnk: SL: Appl:
 0 Quit       Unit0  Inact  no    . Act   . Inact  .     .   insync .
 2            Unit1  Act    no    . Act   . Inact  .     .   insync .
 3
 4
 5
 6
 7 BsyLnk
 8 RTSLnk
 9 SwLnk
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh    SwLnk:    Switch link activity.
  mtc
Time  12:45  >
```

4 This procedure is complete.

—End—

Additional information

Successful completion of the command is indicated with a screen similar to the following.



Changing a user password

The Call Agent platform software load uses the Linux operating system. Use this procedure to change a user password for access to the Call Agent Manager. Changing a user password for access to the call processing application MAP is described in "Performing user administration" (page 74).

Each user can change his or her own password. The root user can change any user's password.

Changing a user password

Step	Action

At the maintenance interface

1 Become the root user with the **su** command.

2 Change the password.

```
# passwd <username>
```

The passwd command provides two prompts to confirm the new password.

```
[root@10.40.44.67 mtc]# passwd mike
syncing password files before attempting operation
Changing password for user mike
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
updating backup password files
[root@10.40.44.67 mtc]#
```

3 This procedure is complete.

—End—

Performing platform user administration

Perform these procedures to add and remove users from access to the Call Agent platform and consequently, the Call Agent Manager. For call processing application user administration, refer to "Performing user administration" (page 74).

Adding a user

Adding a user

Step	Action
	At the maintenance interface
1	Become the root user by using the **su** command.
2	Use the **useradd** command to update the password file. **# useradd <username>**

```
[root@10.40.44.67 mtc]# useradd mike
syncing password files before attempting operation
successfully added user
updating backup password files
[root@10.40.44.67 mtc]#
```

3	Create the user's password. **# passwd <username>** Refer to "Changing a user password" (page 59) for details.
4	This procedure is complete.

—End—

Removing a user

The Linux operating system offers two related commands for restricting access. The first command, **userdel**, completely removes the user from the system. The second option locks the user account, preserves the account information, but prevents log ins.

Removing a user

Step	Action

At the maintenance interface

1 Become the root user by using the **su** command.

2 Delete the user from the password file.

```
# userdel <username>
```

```
[root@10.40.44.67 mtc]# userdel mike
syncing password files before attempting operation
successfully removed user
updating backup password files
[root@10.40.44.67 mtc]#
```

3 This procedure is complete.

—End—

Locking an account

Use this command to maintain the account information, but prevent user log ins.

Locking an account

Step	Action

At the maintenance interface

1 Become the root user by using the **su** command.

2 Lock the account.

```
# passwd -l <username>
```

```
[root@10.40.44.67 mtc]# passwd -l mike
syncing password files before attempting operation
Changing password for user mike
Locking password for user mike
rawpasswd: Success
updating backup password files
[root@10.40.44.67 mtc]#
```

3 This procedure is complete.

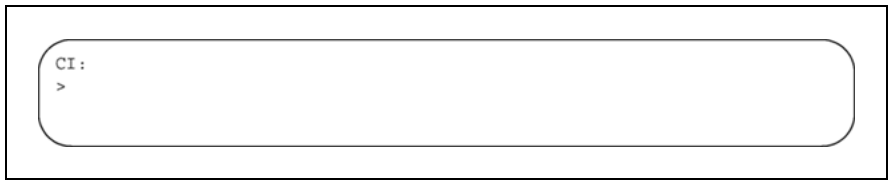
—End—

To unlock the account and restore log ins, use the -u option to the **passwd** command.

MAP Security and Administration

The call processing application provides the MAP interface. The MAP offers many levels and each level offers access to call processing activities. The command interpreter (CI) level of the MAP is used for most security and administration procedures.

The CI is the first level of the MAP available to the user after logging into the CS 2000 Core Manager as "cmusr." Many command driven menus are available from this level.



Performing disk administration

Storage for the Call Agent is provided by pair of STORage Management (STORM) units.

Administration of the storage is completed with the STORM Manager. For information, see *STORM Basics*, NN10024-111.

ATTENTION

Do not modify or manipulate files and volumes through the Call Agent platform shell. Storage and retrieval may be adversely affected.

Use the MAP interface and the commands described in this section for disk, file, and volume administration.

Any files placed within the volume directories from outside the MAP interface must be incorporated into the SOS file system with the DISKUT IMPORT command as soon as possible. Files residing within the SOS volume directories but not registered with the SOS file system may adversely affect volume free space calculations and lead to both service impact and data loss.

Administration of the stored data is available through the call processing application. Three MAP command increments are available for disk administration. Access to these command increments is available from all MAP levels and command increments.

- DISKADM
- DISKUT
- ITOCCI

These disk administration commands are available from all levels of the MAP.

File and volume name expressions

The name expression is a string which specifies the format of the file and volume names. The expression is composed of some of the characters of the intended file/volume names along with special character constructions. The special characters constructions include:

- * - Match any number of characters (including zero) of any type.
- ? - Match exactly one character of any type.
- [ABC...] - Matches one character of those listed between brackets.

  "-" within the left and right braces indicates a range for matching. For example, [AFX-Z135-9] would match one character of: A, F, X, Y, Z, 1, 3, 5, 6, 7, 8, or 9

Whenever one or more of the special characters are used, the entire string must be enclosed in single quotes (apostrophes). As a shortcut, a prefix may be supplied as the name expression rather than including the prefix followed by * and enclosed in quotes. The expression is not case sensitive. For examples and more information, type **Q SCANF** at the MAP.

DISKADM

The disk administration level offers the following commands:

- **BSY**

  Use this command to prevent access to storage. Use the ALL argument during a STORM upgrade.

  ATTENTION
  If the BSY command fails because of open files, first determine the application with the open file. Then use the ROTATE command at the DIRP level to rotate the application from the current disk device to the other disk device.

- **RTS**

  Use this command to re-enable access to storage volumes.

- **DISPLAYDISK (DD)**

  Use this command to display information about the disk device. Important items shown are the number of locked volumes and free space available for new volumes. If a new volume is required and more space is needed, use the STORM Manager to modify the size of the filesystem. If "In Error" is returned as the status for "Device communication," investigate trouble from the STORM Manager.

- **CREATEVOL (CV)**

  Use this command to create another volume on the device.

- **DELETEVOL (DDV)**

  Use this command to delete a volume from the device.

- **DISPLAYVOLS (DV)**

  Use this command to display the volumes on the device, the size of the volumes, the number of Image Table of Contents (ITOC) files on each volume, and the volume path for each volume. If "S" is returned for the volume state, investigate trouble from the STORM Manager.

- **EXTENDVOL (EXV)**

  Use this command to increase the size of a volume. This command fails if the requested size is not available on the disk device.

- **REINITVOL (RV)**

  Use this command to delete all the files in a volume and restore the space from used to available. This command fails if the volume contains load file registered with ITOC or open files.

Examples

The following examples show the syntax for DISKADM commands.

Enter the disk administration level.

Example
>DISKADM device
device
is SD00 or SD01

Busy all volumes on a device. (Volumes with open files cannot be busied. Use the LISTVOLS command in DISKUT to determine the number of open files.)

Example
>BSY ALL

Display the device information.

Example
>DV

```
Information about disk volumes on device SD00.
Volume          Create     Modify     Size  Vol. ITOC  Volume
Name And        Date       Date       Mega- No.  Files Path
State           Y/M/D      Y/M/D      bytes
------------ - ---------- ---------- ----- ---- ----- ---------------
SBA          . 2002/03/08 2002/03/08   400    0     0  /3PC/sd00/sba/
IMAGE        . 2002/03/06 2002/03/06   800    1     1  /3PC/sd00/image/
PERM         . 2001/07/26 2001/07/26   128    2     0  /3PC/sd00/perm/
TEMP         . 2001/11/26 2001/11/26   128    3     0  /3PC/sd00/temp/
IMAGE0       . 2002/03/08 2002/03/08  1024    5     0  /3PC/sd00/image0/
AMA          . 2001/09/25 2001/09/25    63    8     0  /3PC/sd00/ama/
```

Increase the volume size by 50 MB. (DIRP volumes cannot exceed 63 MB.)

Example
>EXV IMAGE 50

Create a volume named TEST with a size of 128 MB.

Example
>CV TEST 128

Delete a volume. (Volumes with ITOC files or open files cannot be deleted.)

Example
>DDV TEMP

DISKUT

The disk utilities level offers many commands. The following list shows frequently used commands:

- **LISTVOLS (LV)**

  Use this command to list all the volumes on all the devices. If "SYSB - Volume is system busy" is returned, investigate trouble from the STORM Manager.

- **LISTFL (LF)**

  Use this command to list the files on a volume. Before a file name can be used as a parameter to another command, the files must be listed with the LISTFL command.

- **DELETEFL (DDF)**

  Use this command to delete a file from a volume.

- **FILEATTR (FA)**

  Use this command to query or set file attributes. Under normal Call Agent operation it should not be necessary to change the attributes for a file.

- **IMPORT**

  Use this command to import single or multiple call processing application images directly from the native file system into the call processing application file system.

  The IMPORT command automatically sets attributes for the imported file based on the following format:

  — *.**<type><num>**' where **<type>** is img, bin, or txt and **<num>** is a one to four digit number expressing the record length in bytes. If the record length for text files is not specified, it may be necessary to use the FA command to set the length.

  — *.txt**<num>**.recs**<num>**' is treated as above, but the second **<num>** is a one to five digit number expressing the file size in records.

  — *$LD' files are imported as LRECL 256 BIN

  — *$PATCH' files are imported as LRECL 128 BIN

  — *_CM' files are imported as LRECL 1020 IMAGE

  — *_MS' files are imported as LRECL 1020 IMAGE

  If the volume name is provided as the only argument to the command, the IMPORT command attempts to import any candidate files in the specified directory, but not already in the volume's file table. For example, if SD00IMAGE is the only argument to the IMPORT command, the command applies the file name expression matching patterns

above, and attempts to import any files in **/3PC/sd00/image** that do not already exist in the file table for the SD00IMAGE volume. When importing image files, note that the syntax is IMPORT **<volume> <filename>** IMAGE 1020.

The IMPORT command ignores candidate files that do not match the file name expression matching patterns above, unless the DEFAULT or OVERRIDE arguments are used. If either if these arguments are used, the file type keyword and associated record length in bytes must be specified. A yes or no prompt is provided for each file entry unless the NOPROMPT argument is used.

Examples

The following examples show the syntax for DISKUT commands.

List the volumes with sizes in MB.

Example

```
>LV MB
```

```
Volumes found:
--------------
NAME            TYPE      TOTAL      FREE TOTAL  OPEN  ITOC    LARGEST
                          MBYTES    MBYTES FILES FILES FILES  FREE SEGMENT
-------------------------------------------------------------------------
SD00IMAGE       STD         1024       229     5     0     0         229
SD00TEMP        STD          256       200    14     0     0         200
```

List the volumes that begin with SD00 in MB.

Example

```
>LV SD00 MB
```

```
Volumes found matching the prefix SD00:
---------------------------------------
NAME            TYPE      TOTAL      FREE TOTAL  OPEN  ITOC    LARGEST
                          MBYTES    MBYTES FILES FILES FILES  FREE SEGMENT
-------------------------------------------------------------------------
SD00IMAGE       STD         800        593     2     0     2         593
SD00IMAGE1      STD         800        581     2     0     1         581
SD00TEMP        STD         200        200     3     0     0         200
SD00PAT         STD         100        100     0     0     0         100
SD00AMA0        STD          64          1   131     0     0           1
SD00AMA1        STD          64          0   128     0     0           0
SD00DLOG        STD          64          1   243     0     0           1
SD00JF          STD          64         49     9     0     0          49
SD00SBA         STD          64         64     0     0     0          64
SD00SCRATCH     STD         100         97    42     0     0          97
SD00SMDR        STD         100          0    48     0     0           0
SD00AMA         STD         300          0    99     0     0           0
SD00OCC1        STD         100          4   159     0     0           4
Total number of volumes matching prefix SD00 : 13.
```

List all image related volumes with sizes specified in MB.

Example

```
>LV '*IM*' MB
```

List SD00TEMP and SD01TEMP.

Example

```
>LV 'SD0?TEMP'
```

List the files in the SD00IMAGE volume. (Sorting options are available for the LF command. Type Q LF for sorting options.)

Example

```
>LF SD00IMAGE
```

```
File information for volume SD00IMAGE:
{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
-------------------------------------------------------------------------------
CSNN06BM_CM              I F           0  1020     195133  388742 011129
.ITOC                    O F           0  1024          1       2 020307
CSNN06AY_CM              I F           0  1020     213853  426036 011213
```

Change the file attributes of a text file to indicate the number of lines in the file.

Example

```
>FA 'fname.txt' SET TEXT_SIZE num
```

fname.txt
is a text file name like **commands.txt**

num
is an integer value less than 65535 and indicates the number of lines in the text file. Use the UNIX word count command, wc, with the lines option, -l (ell), to determine the number of lines in a text file.

Nortel does not support changing attributes on image files.

Import a call processing application image file from **/3PC/sd00/image** into SD00IMAGE. If fname ends in _MS or _CM, specifying the 1020 and IMAGE arguments is unnecessary.

Example

```
IMPORT SD00IMAGE fname IMAGE 1020
```

fname
is the name of the call processing application image file in the native file system

Import all files in the **/3PC/sd00/pmloads** directory into the SD00PMLOADS volume for which the file attributes can be identified and do not already exist in the SD00PMLOADS volume file table.

Example

```
>IMPORT SD00PMLOADS
```

Import a single text file named **ci_script** from the **/3PC/sd01/temp** directory into the SD01TEMP volume.

Example

```
>IMPORT SD01TEMP CI_SCRIPT TEXT 120
```

Import all load files in the **/3PC/sd00/temp** directory into the SD00TEMP volume.

Example

```
>IMPORT SD00TEMP '*LD'
```

Import all file candidates in the **/3PC/sd01/perm** directory into the SD01PERM volume. Files without a file name extension receive a binary type and a record length of 1024 bytes.

Example

```
>IMPORT SD01PERM '*' BIN 1024
```

ITOCCI

The image table of contents command interpreter (ITOCCI) level offers the following commands:

- **LISTBOOTFILE (LBF)**

  Use this command to display the locations and names of files with image file attributes.

- **SETBOOTFILE (SBF)**

  Use this command with the ALR option to set a file for automatic loading.

- **CLEARBOOTFILE (CBF)**

  Use this command to clear the ITOC. This command accepts file names or volume names as arguments. Using file names is the recommended method to prevent loss of data.

- **SETALR (SA)**

  Use this command to set the automatic load option for a file.

Examples

The following examples show the syntax for ITOCCI commands.

If the CS 2000 - Compact is equipped with Message Controller cards, these commands apply to the Message Switch software loads as well. When used for Message Switch loads, the commands use the MS argument instead of the CM argument.

List the boot files.

Example

```
>LBF CM
```

```
Image Table Of Contents:
   A Registered          Generic Device       File
   L Date       Time                          Name
   R MM/DD/YYYY HH:MM:SS
-- - ------------------- -------------------- -----------
 0 * 03/07/2003 21:43:01 SD00IMAGE2           CSNN06BI_CM
```

Enter an additional file to the ITOC.

Example

```
>LF SD00IMAGE

>SBF CM CSNN06BM_CM 1
```

In the example, SD00IMAGE is the name of the volume in which file CSNN06BM_CM exists.

```
Image Table Of Contents:
   A Registered          Generic Device       File
   L Date       Time                          Name
   R MM/DD/YYYY HH:MM:SS
-- - ------------------- -------------------- -----------
 0 * 03/07/2003 21:43:01 SD00IMAGE2           CSNN06BI_CM
 1   03/11/2003 13:18:34 SD00IMAGE            CSNN06BM_CM
```

Clear a file from the ITOC.

Example

```
>LF SD00IMAGE

>CBF CM FILE CSNN06BM_CM
```

In the example, SD00IMAGE is the name of the volume in which file CSNN06BM_CM exists.

Set the automatic load option for a file.

Example

```
>LF SD00IMAGE

>SA CM CSNN06BM_CM
```

In the example, SD00IMAGE is the name of the volume in which file CSNN06BM_CM exists.

All levels

The following disk administration-related commands are available at all levels of the MAP:

- **SCANF**

  Use this command to list files, copy files, and delete files.

  The SORT argument to this command accepts five possible arguments:

  — NAME or BY_NAME to sort alphabetically

— CDATE or BY_CREATE_DATE to sort by creation date

— MDATE or BY_MODIFY_DATE to sort by last modified date

— SIZE or BY_SIZE to sort by file size in blocks

— REV or REVERSE to reverse the order of sorting by NAME, CDATE, MDATE, or SIZE

The SCANF command also accepts a GLOBAL (GS) argument to display the file entries in a single list rather than separate lists based on a volume basis. This argument applies to BRIEF or FULL only.

- **COPY**

Examples

The following examples show the command syntax.

List the files on SD00IMAGE

Example

```
>SCANF SD00IMAGE
```

```
File Index,    Size In    File      Record  File Name
Generation     Records    Attribute Length
(0000 0000)     194678recs -f-i---   1020b  CSNN04BM
(0001 0000)          1recs rf---n-   1024b  .ITOC
(0002 0000)     194938recs -f-i---   1020b  CSNN04AY
(0003 0000)     189998recs -f-i---   1020b  CSNN03BM
```

Delete all the files on SD00TEMP.

Example

```
>SCANF SD00TEMP DELETE NOPROMPT
```

Deleted files cannot be recovered after deletion.

List all the files in the store file device (SFDEV).

Example

```
>SCANF SFDEV
```

Copy a file named BACK14AMA_01 to a file named BACK14AMA_01 and store it on SD01TEMP.

Example

```
>COPY BACK14AMA_01 BACK14AMA_01 SD01TEMP
```

List CM image files, sorted by creation date.

Example

```
>SCANF '*IM*' NAME '*_CM' SORT CDATE GS
```

List all patch files on all TEMP volumes sorted in reverse order.

Example

```
>SCANF '*TEMP' NAME '*$PATCH' SORT NAME REV
```

List all non DIRP segment files on DLOG volumes.

Example

```
>SCANF '*DLG*' NOTNAME 'D*' SORT MDATE GS
```

Performing user administration

User administration allows for adding, deleting, and forcing users off the switch.

Adding a user

The **PERMIT** command has different password restrictions based on enhanced password datafill. The command may request the password and options on different command lines.

Adding a user

Step	Action
	At the MAP terminal
1	Type the following and press the Enter key. **>PERMIT <username>** where <username> is the username *Example system response:* `Enter new password` For the full syntax and available options, type HELP PERMIT at a prompt.
2	Type the user's password and press the Enter key. *Example system response:* `Please enter new password again to verify`
3	Type the user's password and press the Enter key. *Example system response:* `Enter priority, stacksize, language and commandset`
4	Type the following and press the Enter key. **>all**
5	This procedure is complete.

—End—

Deleting a user

Deleting a user

Step	Action
	At the MAP terminal
1	Delete the user. **`>UNPERMIT username`** **`username`** is the system name for the user
2	This procedure is complete.

—End—

Forcing out a user

Forcing out a user

Step	Action
	At the MAP terminal
1	Force the user off the switch. **`>FORCEOUT username`** where <username> is the system name for the user The user can reconnect. Use the UNPERMIT command to prevent the user from logging on again. This command requires administrator privilege.
2	This procedure is complete.

—End—

SAM21 Manager Security and Administration

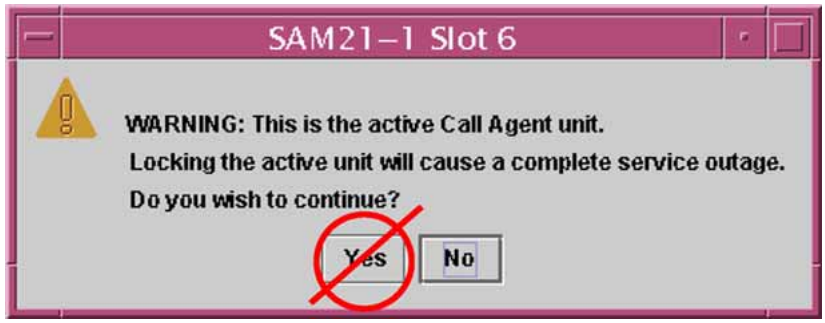
The CS 2000 SAM21 Manager manages the hardware and hardware states of the Call Agent.

Locking the Call Agent

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 prompt show in figure "Call Agent lock warning" (page 77) Do not click Yes. The inactive Call Agent is located in the other CS 2000 SAM21 Manager shelf and a lock request does not provide a prompt when the Call Agent is inactive.

Call Agent lock warning

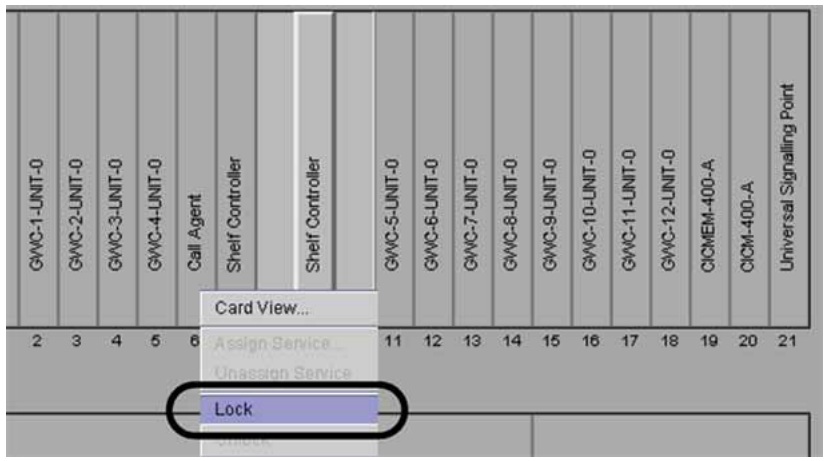


Locking the Call Agent

Step	Action

At the CS 2000 SAM21 Manager client

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



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

2 Do not confirm a lock warning. The warning is only available for the active Call Agent. Wait for the lock icon to appear on the selected card.

3 This procedure is complete.

—End—

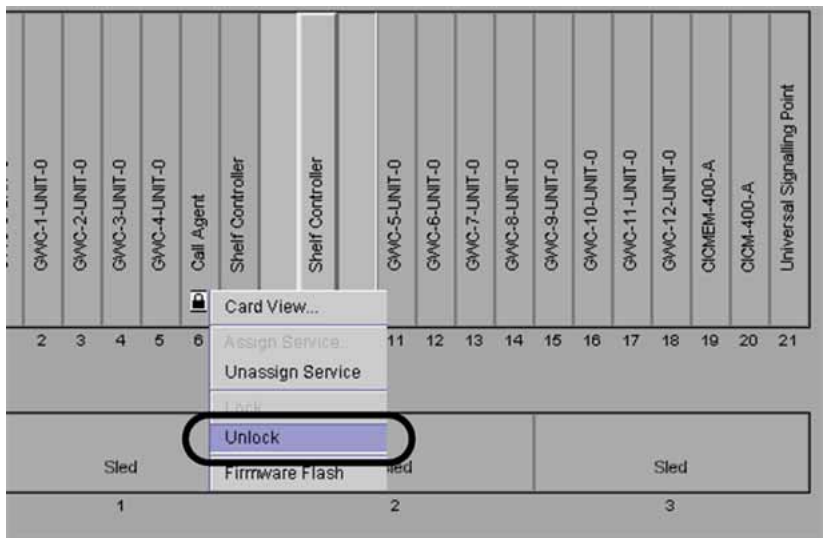
Unlocking the Call Agent

Unlocking the Call Agent

Step	Action

At the CS 2000 SAM21 Manager client

1 From the Shelf View, right click on the card and select Unlock from the context menu.



Unlock is also available from the States tab of the Card View window.

The card resets, downloads software, and reboots.

2 Wait for the lock icon to disappear.

Do not perform any patching activities on the Call Agent until ten minutes have passed.

3 This procedure is complete.

—End—

Message controller

Procedures in this section are related to the security and administration of Message Controller cards.

Administration of the Message Controller cards is completed through two user interfaces. The Call Agent Manager provides an interface for viewing alarms, logs, performance statistics, and controlled shutdown of the card. The CS 2000 SAM21 Manager provides a graphical user interface to complete out of service tasks and initial provisioning.

For offices with Message Controllers, management of the Message Switch software is completed through ITOCCI as with the Call Agent. Refer to "Performing disk administration" (page 64) for information.

Translating ATM links to the Message Switch

Use this procedure to determine the Message Switch, card, and port number termination for an ATM link from the Message Controller. Use this information to busy the ports on the Message Switch before removing a Message Controller from service or when troubleshooting connectivity problems.

Translating ATM links to the Message Switch

Step	Action

At the Call Agent Manager

1 Enter the MCMtc level.

```
MCMtc
```

2 Translate the ATM links on a Message Controller to the termination on the Message Switch.

```
Trnsl <mc_no>
```

mc_no is either 0 or 1

Example

```
Trnsl 0
```

```
 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 Trnsl
 9
10
11           Connectivity report for MC0 retrieved on:
12                Fri Apr  4 10:35:47 2003
13 LogQuery
14 Alarm                                          Cod    Connection
15                              MS   Card  Port  Present    Status
16           ------------------------------------------------------
17 Help      ATM0 connected to:  0     24    0      NO       GOOD
18 Refresh   ATM1 connected to:  1     25    0      NO       GOOD
  mtc
Time  10:35  >  Trnsl 0
```

3 This procedure is complete.

—End—

Querying the sparing link for CCA cards

Use this procedure to find out whether the fiber channel interface or the Gigabit Ethernet interface is currently selected for sparing and synchronizing data between the Compact Call Agent (CCA) cards.

The feature supporting the use of the Gigabit Ethernet interface is applicable only to the CS2100 for the enterprise market.

For detailed information on the fiber channel interface and the Gigabit Ethernet interface, see *Call Agent Basics*, NN10023-111.

Action

If you want to query the sparing link from the SAM21 element manager user interface, see "Querying the sparing link from the SAM21 Manager" (page 83).

If you want to query the sparing link while working in the Call Agent Manager, see "Querying the sparing link from the Call Agent Manager" (page 84).

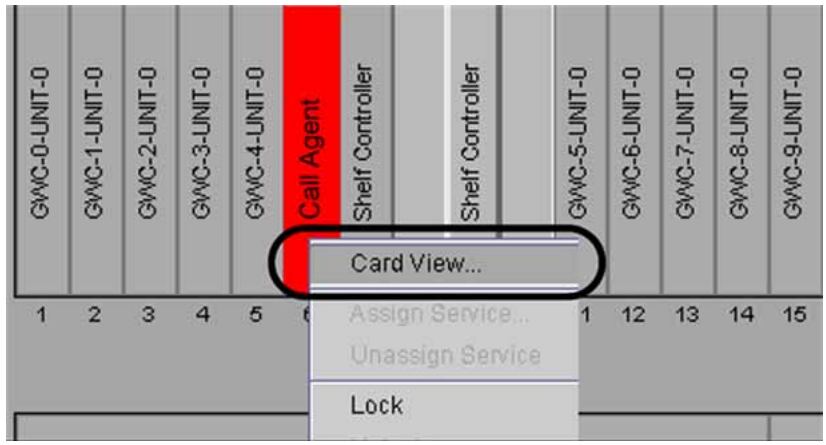
If the currently selected interface is the fiber channel interface, and if you want to migrate to the Gigabit Ethernet interface, contact Nortel.

Querying the sparing link from the SAM21 Manager

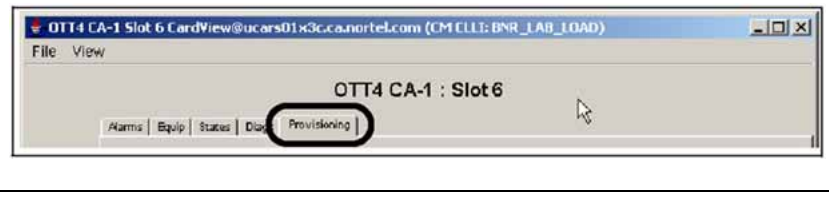
Use the following procedure if you are working in the SAM21 Manager user interface.

Querying the sparing link from the SAM21 Manager

Step	Action
	At the SAM21 Manager client workstation
1	Open the Shelf View of the shelf with the Call Agent card View -> SAM21 Network Element -> 'shelf name'.
2	Right-click on the card icon for the Call Agent card, and select Card View from the context menu to open the Card View window.



3 On the Call Agent Card View window, select the Provisioning tab.



4 On the Provisioning tab select the 'Sparing Link Type' tab.

The 'Sparing Link Type' tab shows a button for each type of sparing link. The currently selected type is highlighted.

5 This procedure is complete.

—End—

Querying the sparing link from the Call Agent Manager

Use the following procedure if you are working at the Call Agent Manager.

Querying the sparing link from the Call Agent Manager

Step	Action

At the Call Agent Manager

1 Enter the CoreMtc level.

```
CoreMtc
```

2 Enter the CAMtc level.

```
CAMtc
```

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

CAMtc                      Jam:  Link0:  Link1:  BLnk: SL: Appl:
 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
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh
  mtc
Time  17:45  >
```

3 Query the sparing link.

QuerySL

In response, the system displays a message identifying the type of sparing-link interface that is currently selected: fiber channel or Gigabit Ethernet.

Examples of system response:

```
Sparing Link (SL) Type:  Fiber Channel
Sparing Link (SL) Type:  Gigabit Ethernet
```

4 This procedure is complete.

—End—

Carrier VoIP

Call Agent Security and Administration

Publication: NN10175-611
Document status: Standard
Document version: 07.02
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

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