MG 9000 Fault Management

New in this release

The following sections detail what is new in MG 9000 Fault Management for release (I)SN09FF.

- Features
- Other changes

Features

The following features appear in (I)SN09FF:

MG9000 Downloadable version of the GLC 32
This feature introduces the NTNY53BA 32-circuit global line card (GLC 32), which can be deployed in either the ATM or IP solution. The NTNY53BA GLC offers field-programmable firmware. Users can upgrade the configuration load of the GLC's Field Programmable Gate Array (FPGA) from the MG 9000 Element Manager (EM). The GLC 32 card replaces the POTS 32 card (the traditional telephone service card with 32 ports). The NTNY53BA GLC can safely replace the GLC NTNY53AA and the WLC 32 without deprovisioning prior to replacement.

Maintenance and card replacement procedures for the NTNY53BA card are the same as those already in use for the NTNY53AA card.

Manufacture of the NTNY53AB GLC 32 card has been discontinued. References to the NTNY53AB card have been removed from this publication.

MG9000 GLC 12 Line Card providing NA Coin services
This feature introduces the NTNY53CA 12-circuit global line card (GLC 12), which can be deployed in either the ATM or IP solution. The GLC 12 is based on existing GLC 32 technology line card and is functionally identical to the NTNY53BA GLC 32, but with the addition of support for native Coin Lines. The GLC 12 supports all line service types supported by existing MG 9000 line cards.

The GLC 12 replaces the Service Adaptive Access 12-circuit line card (SAA 12). The NTNY53CA 12-line GLC can only safely replace the SAA-12 card without deprovisioning prior to replacement. The software to support the card is patched back to SN08.

Maintenance and card replacement procedures for the NTNY53CA card are the same as those already in use for the NTNY53AA card.

Global Line Card Field Programmable Gate Array Download
This feature provides the software interface for the downloadable NTNY53CA GLC 12 and NTNY53BA GLC 32 cards. Changes appear in the GLC Card View that allow users to access the Software Download Manager, and to view the FPGA configuration load of a selected card. The MG 9000 Upgrade Wizard, the interface used to upgrade the firmware, has also been modified to include the GLC cards.

This feature also introduces a new GLC Circuit Controller Diagnostic test to determine if a circuit requires reloading. The GLC Circuit Controller Diagnostic test appears in the pick list along with other diagnostic tools available from the MG 9000 Diagnostic View.

PKI authentication on the MG9K (phase 1)
This feature introduces enhancements to the way security keys are managed when used with IP Security (IPSec) on the MG 9000 gateway and its collaborating peers.

This feature adopts Public Key Infrastructure (PKI) to manage the generation and distribution of keys used to authenticate nodes participating in an IPSec session.

PKI is a widely used standard supporting the generation, distribution and redistribution of keys. This feature addresses the reception, installation and use of digital certificate authenticate nodes attempting to establish an IPSec session.

MG 9000 Manager Capacity Performance Robustness (CPR) simplification
Clear persist and discover operations can be launched from the MG 9000 Manager through a new button on the NE Discovery View window.

Other changes

There are no other changes in the (I)SN09FF release.

Fault management strategy

Faults on the MG 9000 or any component in the frame or shelf are reported as alarms to the MG 9000 Manager. In addition, some frame and shelf alarms are reported to the alarm indicators on the Intelligent Bay Interface Panel (IBIP) and to the office alarm unit (OAU).

Tools and utilities

The following interfaces are used to install, commission, and maintain the MG 9000. These interfaces are described next.

- local craft interface (LCI)
- MG 9000 Manager graphical user interface (GUI)

Local craft interface

The LCI provides MG 9000 management through a Netscape or Internet Explorer browser on a laptop personal computer (PC). The network server uses Hypertext Transfer Protocol (HTTP) to send Hypertext Markup Language (HTML) to the browser. This form of network management allows a PC-based browser to display statistics and control and configure a network device. The LCI runs off the active Data Control Card (DCC) on the MG 9000.

The LCI is used for initial commissioning and in emergency instances when the MG 9000 Manager is not available. Daily operation, administration, and maintenance of the MG 9000 is performed from the MG 9000 Manager. The LCI runs with Internet Explorer 5.5 or Netscape 7 on Windows2000 (versions of Netscape between NN4.7 and NN7 are not supported). Netscape 4.7 is being supported for any users still having Windows95 operating systems.

For more information on the LCI, refer to *MG 9000 Configuration Management*, NN10096-511.

MG 9000 Manager graphical user interface

The MG 9000 Manager serves as the element management system for the MG 9000 within a Carrier VoIP Network. The MG 9000 Manager enables remote management of multiple MG 9000 network elements through a single GUI. The MG 9000 Manager is a server/client application that runs on a Unix-based workstation or a PC-based client application.

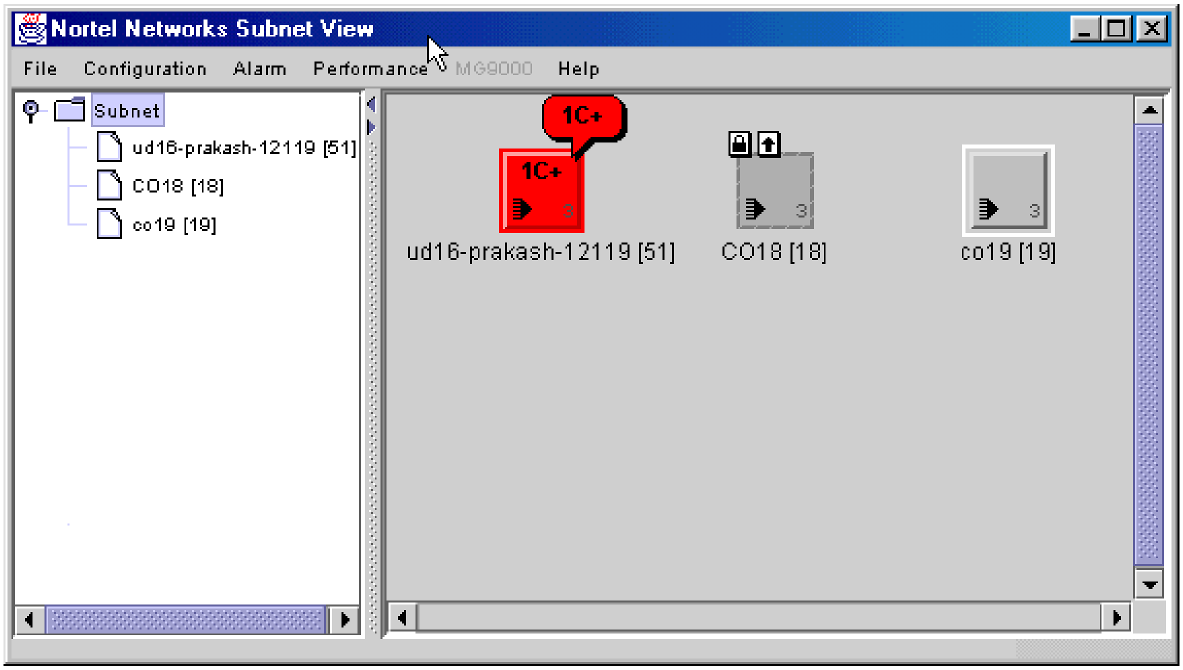
The MG 9000 Manager manages the MG 9000, dealing with operation/issues that affect the network element, such as

- network element discovery
- equipment provisioning

- carrier provisioning
- service provisioning (network element [NE] specific commands)
- fault handling and reporting

The following figure shows the window-based MG 9000 Manager Subnet View. In this figure, the icon in solid grey without diagonal lines indicates that the MG 9000 is provisioned and discovered. In the Subnet View. A tree view is available in the left side. Each entry or 'NE' in the tree indicates the presence of some entity. The top node (also known as the root NE) indicates the subnet itself, and is named accordingly; its icon shows a folder to indicate it (may) contain other items. As MG 9000s are added to the subnet, they will appear as additional NEs in the tree, connected by a line to the root 'subnet' NE. This indicates a containment relationship that the subnet has over its constituent MG 9000s.

MG 9000 Manager Subnet View



Each MG 9000 NE is shown as a standard 'paper' icon, to indicate there is information available about that particular MG 9000 at this level of the tree. The icon is accompanied by the name of the MG9000, and its network element number appended in square brackets.

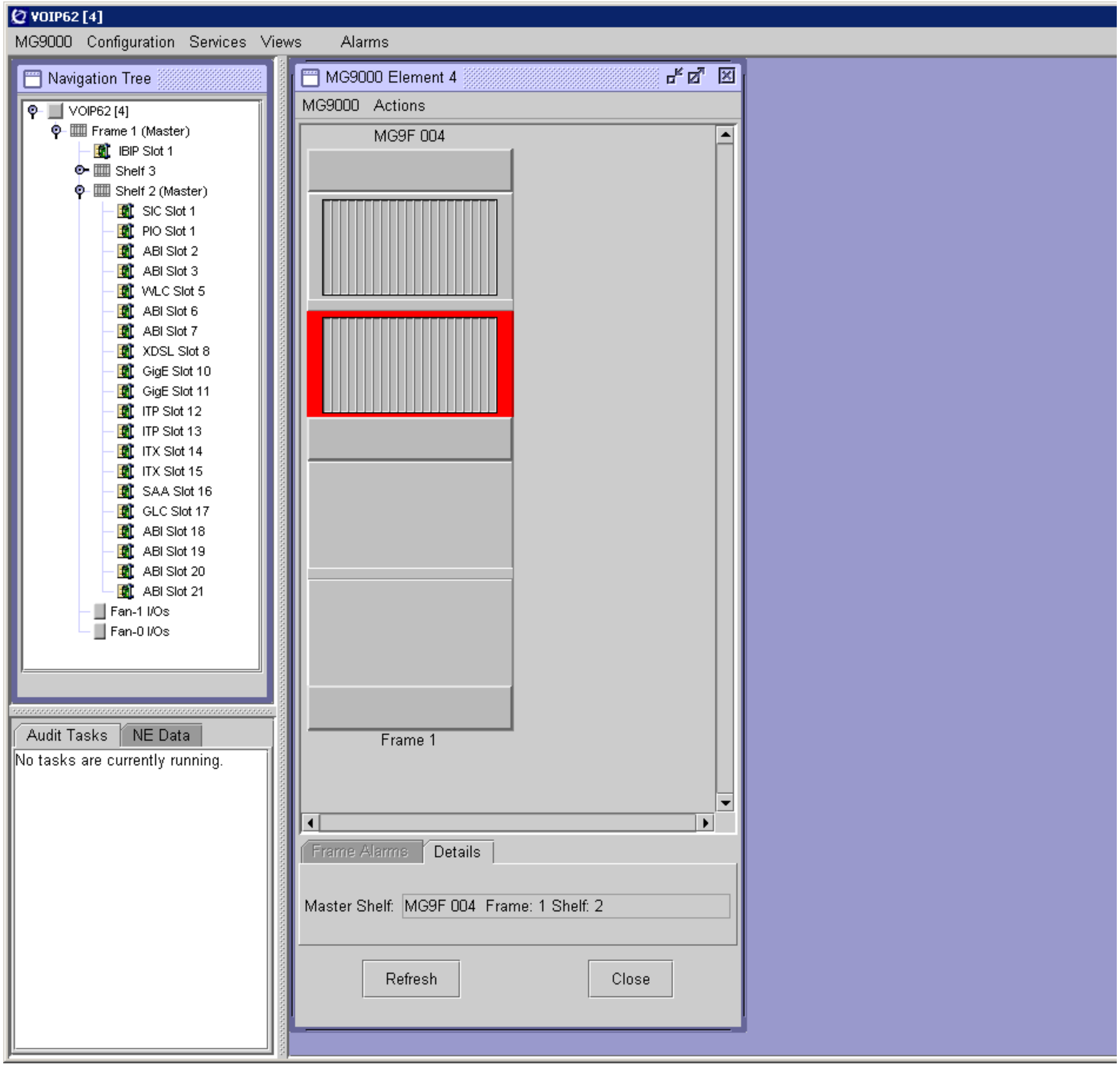
> ***Note:*** During the initialization of the MG 9000, the explanatory text may show an internal network identifier and 'Unknown' until the MG 9000 has been created.

The user may click on the MG 9000 NEs listed in the tree; doing so will result in a purple selection bar appearing around the explanatory text to indicate this is the current MG 9000 in selection. At the same time, the corresponding icon in the network view will also be selected. Clicking on an MG 9000 icon in the Subnet View results in the selection bar appearing in the tree view, meaning the two views are synchronized together.

To launch the Frame View for an MG 9000, double-click on the MG 9000 item in the tree view. If the MG 9000 is not in a state where the Frame View can be displayed, a warning may appear. When double-clicking on the NE icon or the NE in the tree view, a NE desktop view appears for each network element and the Frame View and all subtending GUIs appear in that desktop view. The next figure shows the Frame View within the NE desktop view. At the left side of the NE desktop view is a Navigation Tree showing the network element, each frame in the NE, the IBIP shelf, the master shelf, any subtending shelves, and fan shelves. When the user double clicks on the shelves, the tree view is expanded to show the cards in each slot and the shelf view for that shelf appears. When the user double clicks on any card in the tree view, the card view appears.

The Audit Task tab shows the progress of an NE audit and is meant as an audit indicator for those tasks that run in the background so the user is aware that an NE audit is currently in progress. Throughout this document, the individual GUIs are shown outside the NE desktop view, though in all cases except for the Alarm Browser, the GUIs appear in the NE desktop view.

Frame View shown within NE desktop view



No tasks are currently running.

Master Shelf: MG9F 004 Frame: 1 Shelf: 2

The menu bar across the top of the NE desktop view consists of the following menu items

- Configuration - contains menu items Add new MG9000 NE, Audit NE, Delete NE, Discover NE, View/Modify NE Properties, Refresh

Icon and Launch LCI Session which are described in *MG 9000 Configuration Management*, NN10096-511

- Services - contains menu items
  - Bandwidth Manager, Private Lines Services Manager, and Switched Lines Services Manager which are described in *MG 9000 Configuration Management*, NN10096-511
  - DTA Test Manager and MTAP Test Manager, which are described in Testing lines
  - Floating IP Address Manager, which is described in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450
- Views - lists the open views within the NE desktop provides for easy retrieval of views that are nested
- Alarms - contains Alarm Browser which is described in Alarm Browser and Audit NE Alarms described in Audit NE alarms

Each GUI within the NE desktop view can be maximized or minimized within the NE desktop view, similar to how windows can be manipulated in a Windows PC desktop. When the last GUI is closed, the NE desktop view automatically closes.

Currently, clicking on the Subnet root icon has no function. The tree may also be expanded/reduced by clicking on the handle icon in the upper left hand corner of the tree view. Expanding the tree shows all the MG 9000s in the subnet. Reducing the tree removes the NEs from the display. These are only hidden for display purposes, they are not removed from the network.

When a network element has more than one subtending frame, the frames appear together in the Frame View without a gap, even though in the office line up the frames may be separated. In the MG 9000 Manager, the master frame is shown to the left in the Frame View with subtending frames shown to the right shown in order of their internal frame number.

MG 9000 Manager user inactivity timeouts

The following configurable user inactivity timeouts apply to the MG 9000 Manager:

- User Inactivity Timeout (Default: 10 minutes)
- User Termination Timeout (Default: 10 minutes)
- Re-Authentication Disable Timeout (Default: 30 seconds)

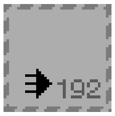
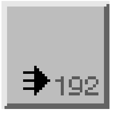
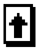
After the user launches the MG 9000 Manager client GUI, if there is no user initiated client-server interaction for the duration of the first timer (User Inactivity Timeout), the GUI is iconized and a dialog appears prompting the user to re-login. Only after successful re-authentication is the GUI de-iconized. If there is no user initiated client-server interaction for the duration of the second timer (User Termination Timeout), a dialog appears warning the user that the client is locked because of extended inactivity. When the user confirms the message, the client and the login dialog GUI are closed.

> ***Note:*** For HA cluster systems, timeout values are set independently for each side of the cluster. If timeout values have only been changed on the active side of a cluster and a SWACT occurs, the timeout values will take the inactive side settings. To ensure consistent interface performance following a SWACT, when a default timeout setting is changed on the active side of the cluster, the corresponding setting should also be changed on the inactive side of the cluster. Refer to the chapter on modifying login session timeouts on the CS 2000 Management Tools server, in *ATM/IP Security and Administration* (NN10402-600).

MG 9000 Manager icons

The following table identifies the icons used in the MG 9000 Manager to report the node states, alarms, and status. The first two icons in the table depict a network element. The icons that follow in the table are used to identify the procedural, availability, and control status of the MG 9000. Wherever these icons appear, the technician can move the mouse to place the cursor over the icon and a information balloon will appear showing the icon name as presented in the second column of the following table. These icons are also used to identify the state, availability, and status of nodes on the MG 9000 shelf.

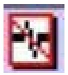
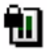
MG 9000 Manager operational, state, and status icons

Icon	Icon name	Purpose
	N/A	MG 9000 network element has been added or pre-provisioned at the EM but is not yet discovered.
	N/A	MG 9000 network element has been discovered and is ready for use.
	Network element not discovered	Network element has not sent initial “cold start” TRAP to EM.
	Network element discovery or card initialization in progress	Network element has sent “cold start” TRAP and the EM is reading hardware information.
	Inhibit in Progress	Going out of service.
	Degraded	Service is degraded. This could adversely affect the usage state.
	Failed	Network element discovery failed, either during hardware or services data upload.
	In test	Resource is undergoing test.
	Backup card present	A backup resource is available.

MG 9000 Manager operational, state, and status icons

Icon	Icon name	Purpose
⬇	Software download	Software downloading activity is being performed on this card.
☒	Test failed	The card has failed diagnostic test.
☑	Test passed	The card has passed diagnostic test
🔒	Locked	The Administrative State for this card is set to Locked or NE not discovered.
☒	APS Failure	APS failed on the OC-3 network interface
⟳	Active card	The card is active
W	Working	The redundant (slave) ABI (DS-512) card is providing service
⧉	No Spare or backup card present	A backup resource is not available
🚫	Power Off	The card has lost power
🕒	Off duty	The card is not in service
⚡	High voltage	Over voltage condition detected on WLC card

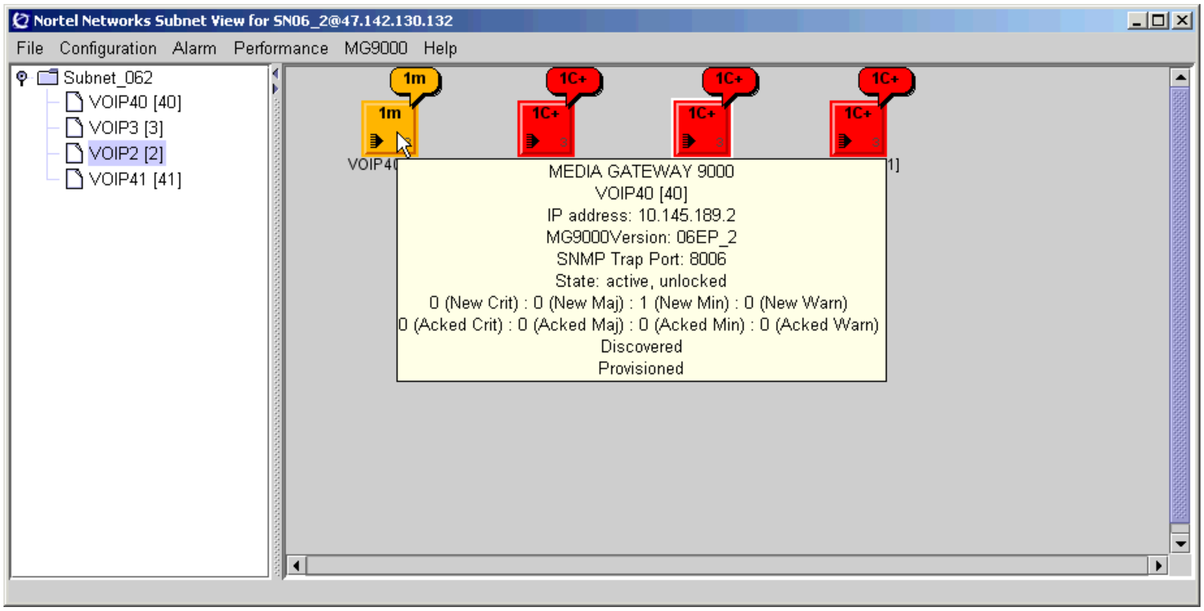
MG 9000 Manager operational, state, and status icons

Icon	Icon name	Purpose
	Emergency stand alone (ESA) - appears in the Switched Lines Services View	Identifies a virtual media gateway (VMG) is in ESA mode. Seen in the Switched Lines Services GUI.
	NE status icon	Indicates an MG 9000 is provisioned but is no longer managed by the MG 9000 Manager. This may occur when an MG 9000 that was managed by an MG 9000 Manager running at SN06.2 is now managed by an MG 9000 Manager running at SN08. The traps are now being reported to a different IP address and port that is not the same as its own SNMP listening port. After upgrading to SN08, the MG 9000 Manager’s SNMP listening port is 8002.

In the following figure, the Subnet View is shown along with the information balloon for the network element over which the cursor has been placed. The balloon appears for approximately 5 seconds then disappears and will reappear each time the cursor is moved over the NE. The information balloon provides the following:

- network element name and number
- MG 9000 software release
- network element IP address
- SNMP trap port number used
- state of the network element
- total alarms by category and the number of alarms that have been acknowledged

Subnet View showing the information balloon

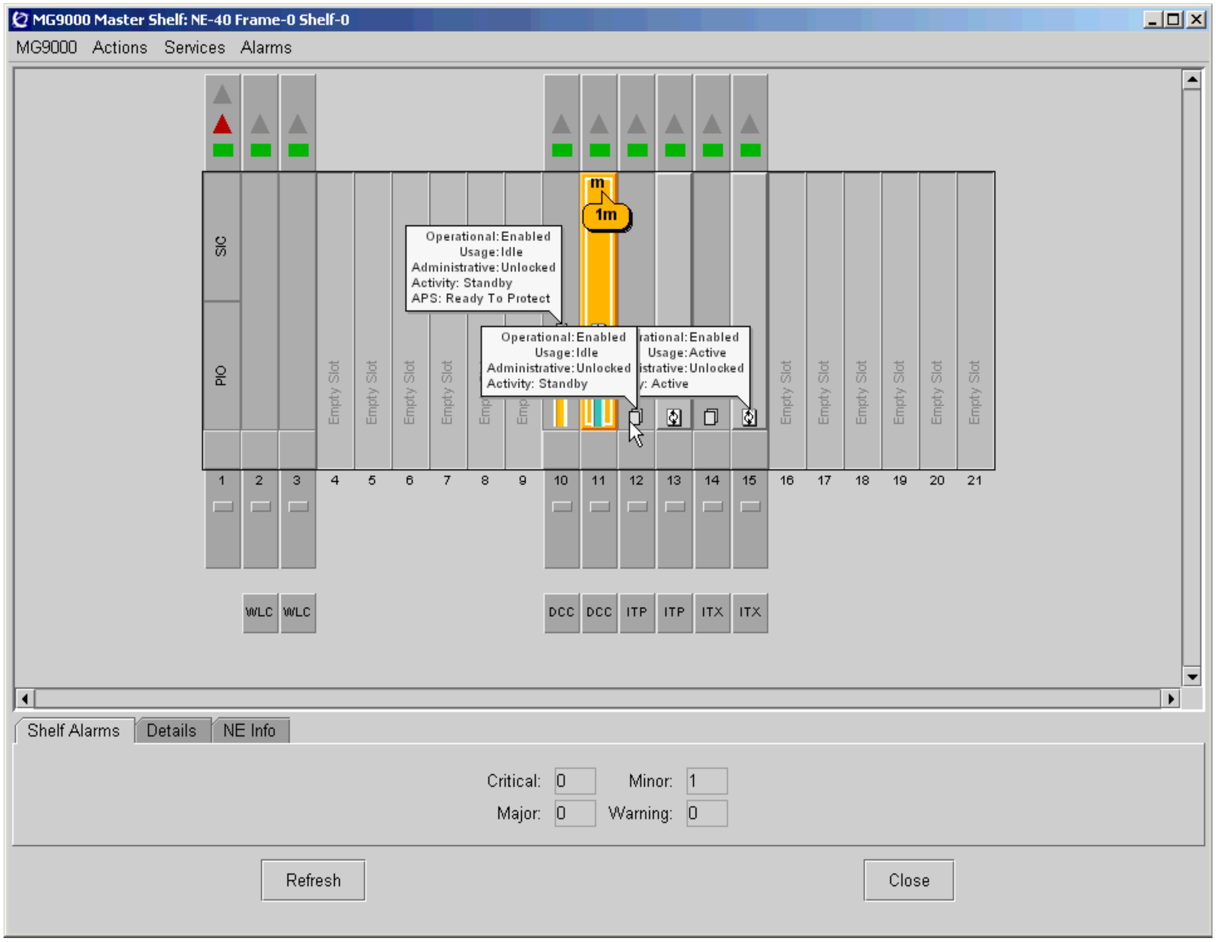

Nortel Networks Subnet View for SN06_2@47.142.130.132
File Configuration Alarm Performance MG9000 Help
Subnet_062
VOIP40 [40]
VOIP3 [3]
VOIP2 [2]
VOIP41 [41]
1m
1C+
1C+
1C+
VOIP4
1]

MEDIA GATEWAY 9000
VOIP40 [40]
IP address: 10.145.189.2
MG9000Version: 06EP_2
SNMP Trap Port: 8006
State: active, unlocked
0 (New Crit) : 0 (New Maj) : 1 (New Min) : 0 (New Warn)
0 (Acked Crit) : 0 (Acked Maj) : 0 (Acked Min) : 0 (Acked Warn)
Discovered
Provisioned

In the Shelf View, by placing the cursor over the icon and clicking once on each card, the technician can retrieve information about the state of that card and link. The following figure shows the information balloon. To remove the balloon, click once again on the icon. The following information appears in the balloon:

- operational state
- card status
- card availability
- activity status
- link status

Shelf View with information balloons



MG9000 Master Shelf: NE-40 Frame-0 Shelf-0

Operational:Enabled
Usage:Idle
Administrative:Unlocked
Activity: Standby
APS: Ready To Protect

Operational:Enabled
Usage:Idle
Administrative:Unlocked
Activity: Standby

rational:Enabled
Usage:Active
istrative:Unlocked
/: Active

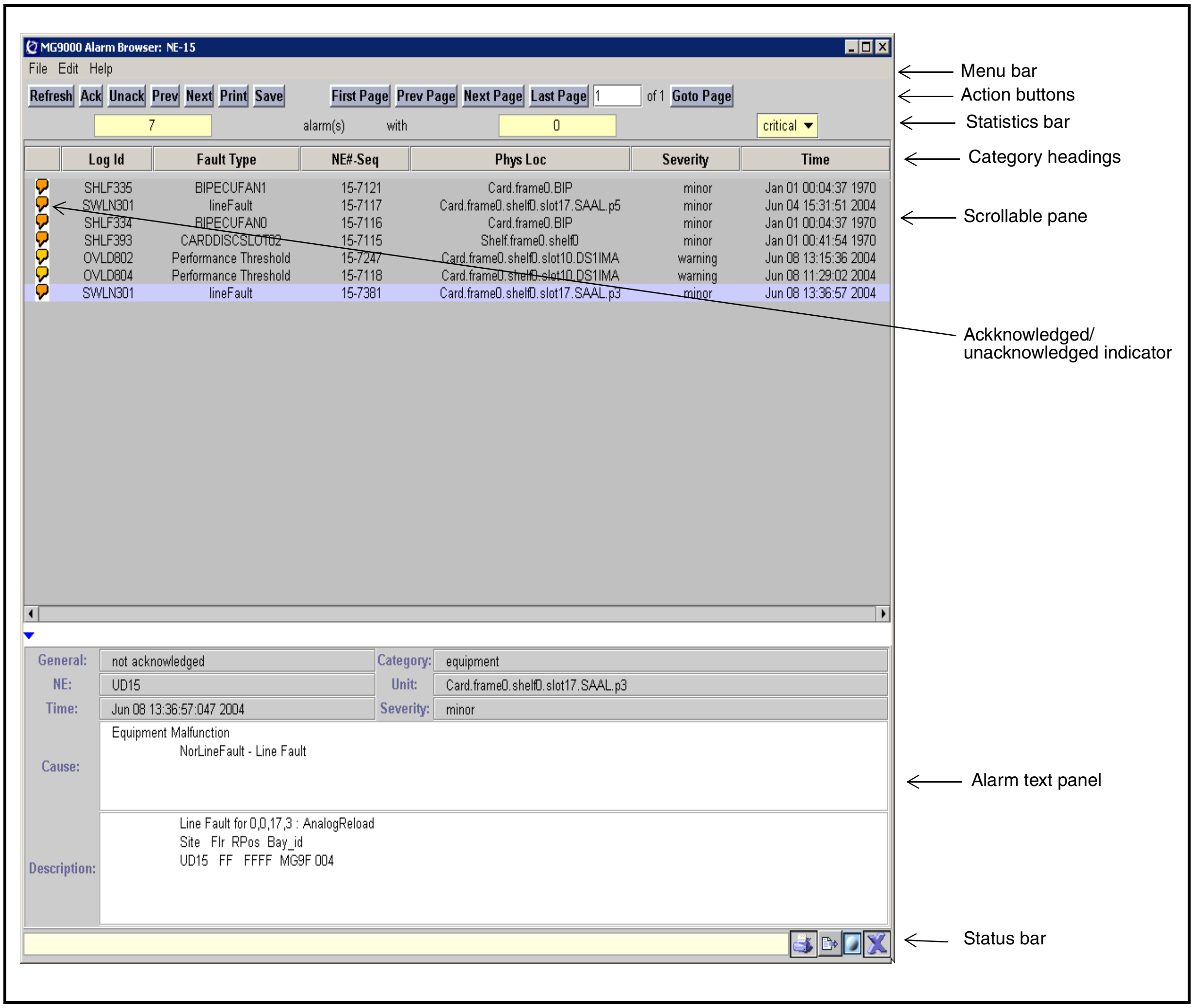
Critical: 0 Minor: 1
Major: 0 Warning: 0

Alarm Browser
The Alarm Browser screen is used for alarm surveillance. The Alarm Browser screen is accessed from the “Alarm” menu option at the top of all screens. The Alarm Browser consists of multiple sections used to view and manage MG 9000 alarms. Once the alarm browser is open, the browser continues to update as new alarms are added or conditions change.

When multiple Alarm Browser screens are open on the same MG 9000 Manager, the frame title of the Alarm Browser contains the network element number to clearly relate the Alarm Browser with the network element for which alarms are being monitored.

The following figure shows the Alarm Browser screen.

Alarm Browser



MG9000 Alarm Browser: NE-15

7 alarm(s) with 0 critical

	Log Id	Fault Type	NE#-Seq	Phys Loc	Severity	Time
●	SHLF335	BIPECUFAN1	15-7121	Card.frame0.BIP	minor	Jan 01 00:04:37 1970
●	SWLN301	lineFault	15-7117	Card.frame0.shelf0.slot17.SAAL.p5	minor	Jun 04 15:31:51 2004
●	SHLF334	BIPECUFAN0	15-7116	Card.frame0.BIP	minor	Jan 01 00:04:37 1970
●	SHLF393	CARDDISCSLOT02	15-7115	Shelf.frame0.shelf0	minor	Jan 01 00:41:54 1970
●	OVLD802	Performance Threshold	15-7247	Card.frame0.shelf0.slot10.DS1IMA	warning	Jun 08 13:15:36 2004
●	OVLD804	Performance Threshold	15-7118	Card.frame0.shelf0.slot10.DS1IMA	warning	Jun 08 11:29:02 2004
●	SWLN301	lineFault	15-7381	Card.frame0.shelf0.slot17.SAAL.p3	minor	Jun 08 13:36:57 2004

General: not acknowledged
Category: equipment
NE: UD15
Unit: Card.frame0.shelf0.slot17.SAAL.p3
Time: Jun 08 13:36:57:047 2004
Severity: minor

Cause:
```
Equipment Malfunction
        NorLineFault - Line Fault
```

Description:
```
        Line Fault for 0,0,17,3 : AnalogReload
        Site  Flr  RPos  Bay_id
        UD15   FF   FFFF  MG9F 004
```

The following table lists the menu bar options.

Alarm Browser menu bar

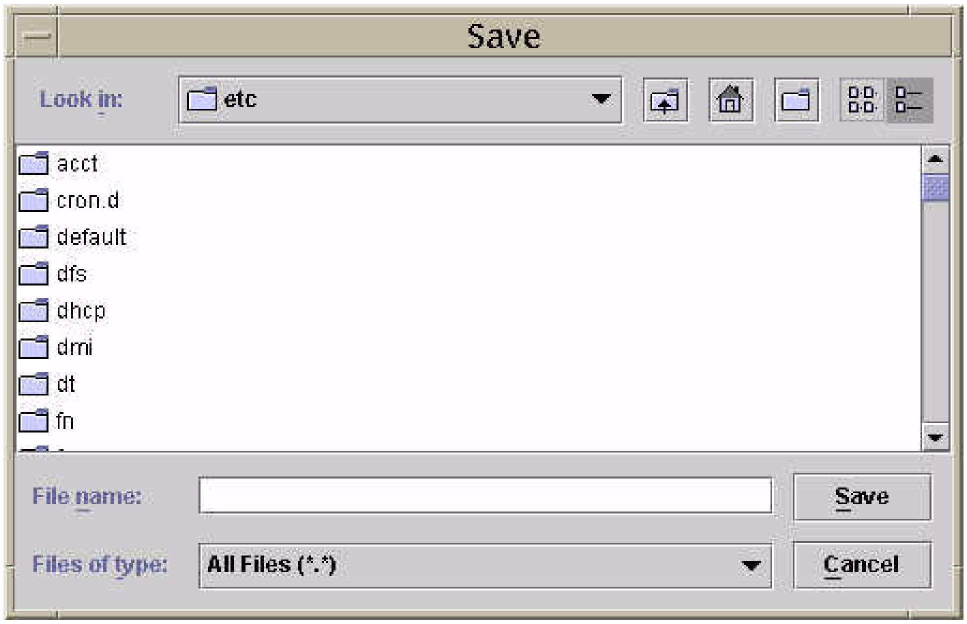
Menu Item	Option	Explanation
File	Refresh	Refreshes alarm from the MG 9000 Manager server into the presentation window.
	Save	Saves a text format of the alarm information in the presentation window to a file.

Alarm Browser menu bar

Menu Item	Option	Explanation
	Print	Prints a text format of the alarm information in the presentation window.
	Exit	Closes the Alarm Browser screen
Edit	Presentation Preferences	Used to define the category headings used on the Alarm Browser.

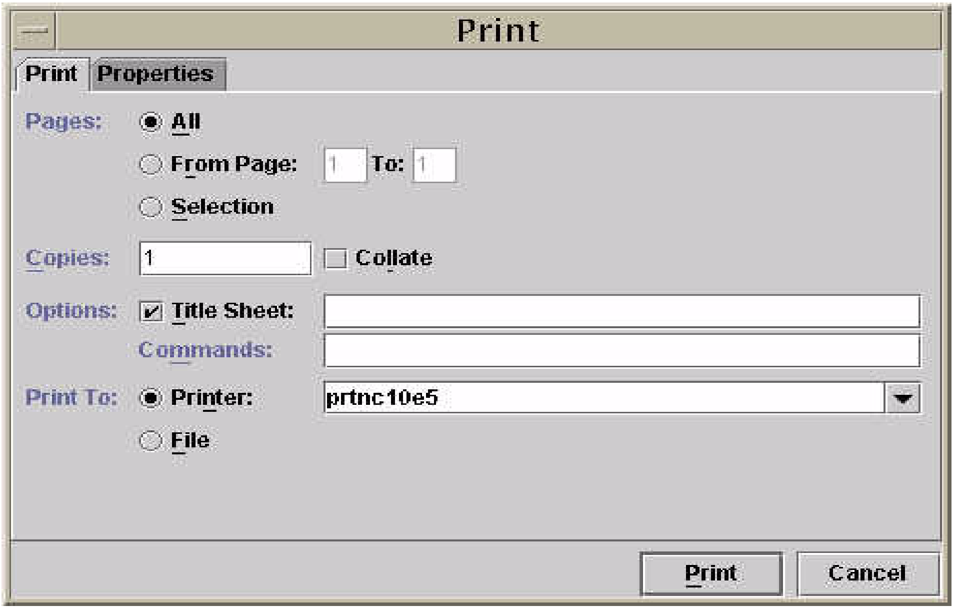
The following figure shows the Save dialog screen.

Alarm Browser Save dialog screen



The following figure shows the Print dialog screen.

Alarm Browser Print dialog screen



Pages: ● All
○ From Page: 1 To: 1
○ Selection

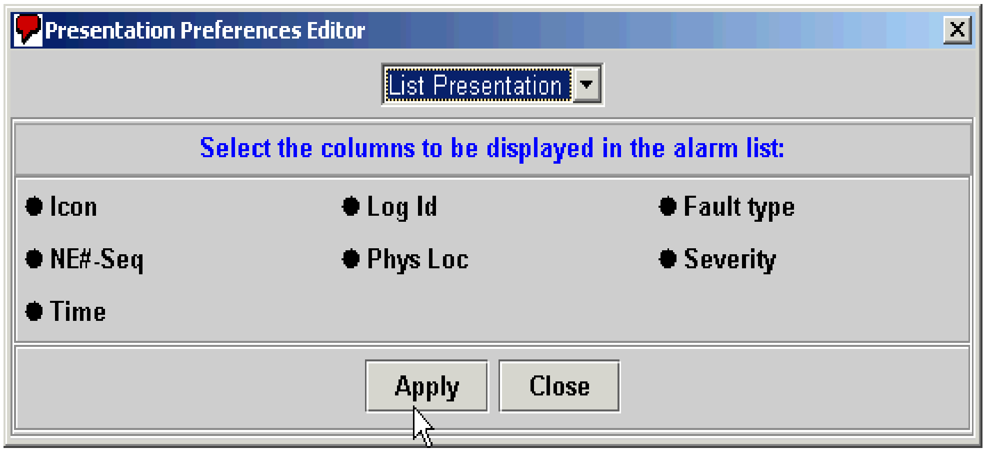
Copies: 1 □ Collate

Options: ☑ Title Sheet:
Commands:

Print To: ● Printer: prtnc10e5
○ File

The Category Headings table describes the headings listed on the List Presentation decision screen.

Alarm Browser List Presentation Editor



Select the columns to be displayed in the alarm list:

● Icon ● Log Id ● Fault type
● NE#-Seq ● Phys Loc ● Severity
● Time

Click on a radio button next to a category to either select or deselect the category. Click on “Apply” to accept the change.

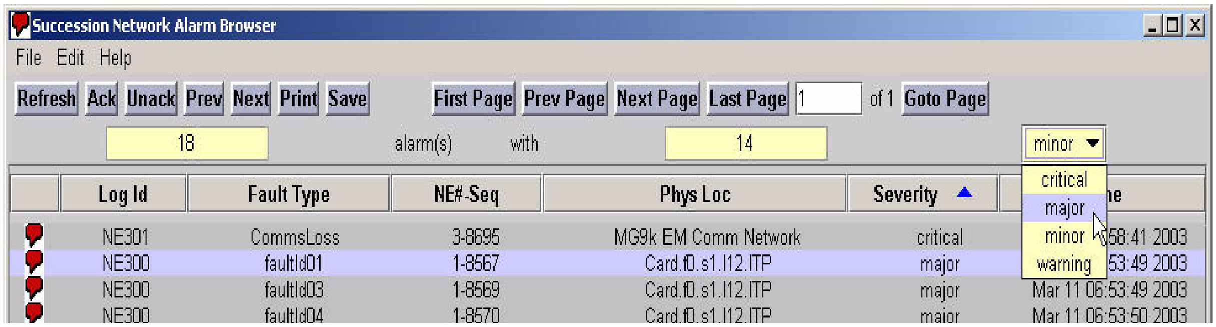
The Action Buttons located immediately below the Menu bar in the Alarm Browser, provide Alarm Browser screen management options. The following table lists the Action Buttons on the Alarm Browser.

Action Buttons

Button	Explanation
Refresh	Refreshes the alarms from the MG 9000 Manager server.
Ack	Acknowledged. An acknowledged alarm indicates the alarm has been seen and provides the option to visually distinguish which alarms have been addressed. An acknowledgement causes the alarm notification in the presentation area to change from a solid color to an empty fill.
Unack	Unacknowledged. Removes an acknowledge from an alarm and changes the alarm notification to a solid fill. The unacknowledged option provides a method of changing an alarm back to a higher priority.
Next	Moves the selection highlight to the alarm below the current selected alarm.
Prev	Previous. Moves the selection highlight to the alarm above the current selected alarm.
Print	Prints the alarm information in the presentation window.
Save	Saves the alarm information in the presentation window to a file.
First page	When multiple pages of alarms are present, allows the user to go to the first page of alarms.
Prev page	When multiple pages of alarms are present, allows the user to go to the previous page of alarms.
Next page	When multiple pages of alarms are present, allows the user to go the next page of alarms.
Last page	When multiple pages of alarms are present, allows the user to go the last page of alarms.
Goto page	When multiple pages of alarms are present, allows the user to go to a specific page number in the pages of alarms available.

The Statistics Bar summarizes the total number of alarms in the scrollable pane and within that total, the number of a selected alarm type. The selected alarm type isolated in the summary can be selected from any of the available alarm types. For example, the following figure shows a Statistics Bar indicating that the scrollable pane has 20 alarms with one critical alarm. In the figure, the box to change alarm types is open and ready for selection.

Statistics Bar



18 alarm(s) with 14 minor

	Log Id	Fault Type	NE#-Seq	Phys Loc	Severity	ne
	NE301	CommsLoss	3-8695	MG9k EM Comm Network	critical	58:41 2003
	NE300	faultId01	1-8567	Card.f0.s1.I12.ITP	major	53:49 2003
	NE300	faultId03	1-8569	Card.f0.s1.I12.ITP	major	Mar 11 06:53:49 2003
	NE300	faultId04	1-8570	Card.f0.s1.I12.ITP	major	Mar 11 06:53:50 2003

The Category Headings define the columns of data that appear in the Alarm Browser. The Edit menu option configures which headings appear on the browser. The following table lists all of the possible headings that can appear on the browser.

Category Headings

Field	Explanation
<no field title>	An icon presentation determining if an alarm has been acknowledged. • solid fill for unacknowledged alarms • empty fill for acknowledged alarms
Log id	Log report number associated with the alarm
Fault Type	Specific type of fault that caused the alarm
NE#-Seq	Two numbers separated by a hyphen used to identify the alarm in the browser and the MG 9000 source. • the first number represents the network element (MG 9000) number in the network • the second number is the sequential number of the alarm on the browser screen
Phys. Loc	Identifies the MG 9000 component hardware source of the alarm.

Category Headings

Field	Explanation
Severity	The alarm severity: • critical • major • minor • warning
Time	The time that the alarm occurred. The time is displayed in the following format: mmm dd hh:mm:ss year For example: Feb 28 06:04:45 2001

The Alarm Text Panel contains a text summary of a selected alarm highlighted in the scrollable pane. The following table lists the fields in the Alarm Text Panel.

Alarm Text Panel

Field	Explanation
General	A text summary of the alarm status.
NE	The name assigned to the MG 9000.
Time	The time that the alarm occurred. The time is displayed in the following format: mm dd hh:mm:ss year For example: Feb 28 06:04:45 2002
Category	The category of the component affected by the fault.
Unit	The component type, and location of the alarm, where: • f = frame • s = shelf • l = slot • p = port For example, the text “Port.f1.s3.l7.DS1.p0” indicates, a port problem in MG 9000 frame 1, shelf 3, slot 7, at DS1 port 0.

Alarm Text Panel

Field	Explanation
Severity	The alarm severity: • critical • major • minor
Cause	Indicates the cause of the alarm.
Description	A brief description of the type of error and cause. The location of the faulty component as: Site, Floor, RPos, and Bay_id ***Note:*** Default Fs appear in this field until frame location information is provisioned for the master shelf and subtending frames. When frame location information is provisioned for the frames, alarms reported on components in the frame are reported with the frame location information. For information on provisioning the frame location information, refer to procedure “Provisioning an MG 9000 frame’s physical location” in *MG 9000 Configuration Management*, NN10096-511. The directory number (DN) is shown for line circuit alarms. If no DN exists for the affected line circuit, the description field reads “DN affected: None.” ***Note:*** After the line circuit alarm is reported to the Alarm Browser, any subsequent changes to the DN of that particular line circuit are not updated in the description part of the Alarm Browser for a line circuit alarm. However, when alarms are audited, any changes done to the DN of that particular line circuit after an alarm is raised are updated in the description part of the Alarm Browser for a line circuit alarm.

The status bar at the bottom of the Alarm Browser screen serves two functions:

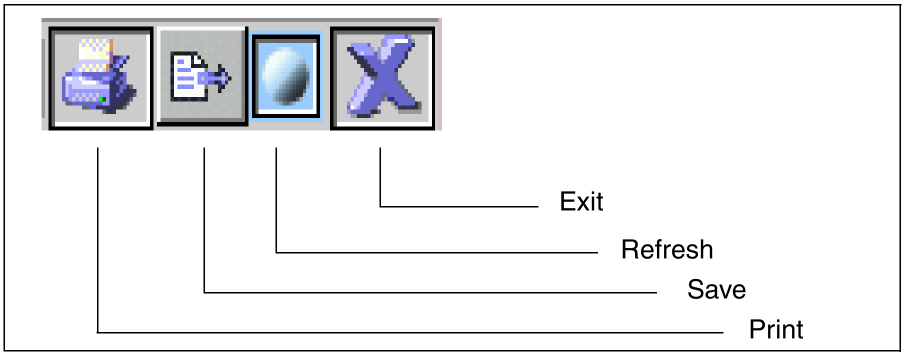
- an alarm status summary
- icon file options

The summary status indicates

- the number of total alarms when the Refresh button is clicked
- the number of acknowledged/unacknowledged alarms (not currently supported)

The icons on the status bar provide access to some of the features in the File menu. The following figure shows the status bar icons and their functions.

Status Bar icons



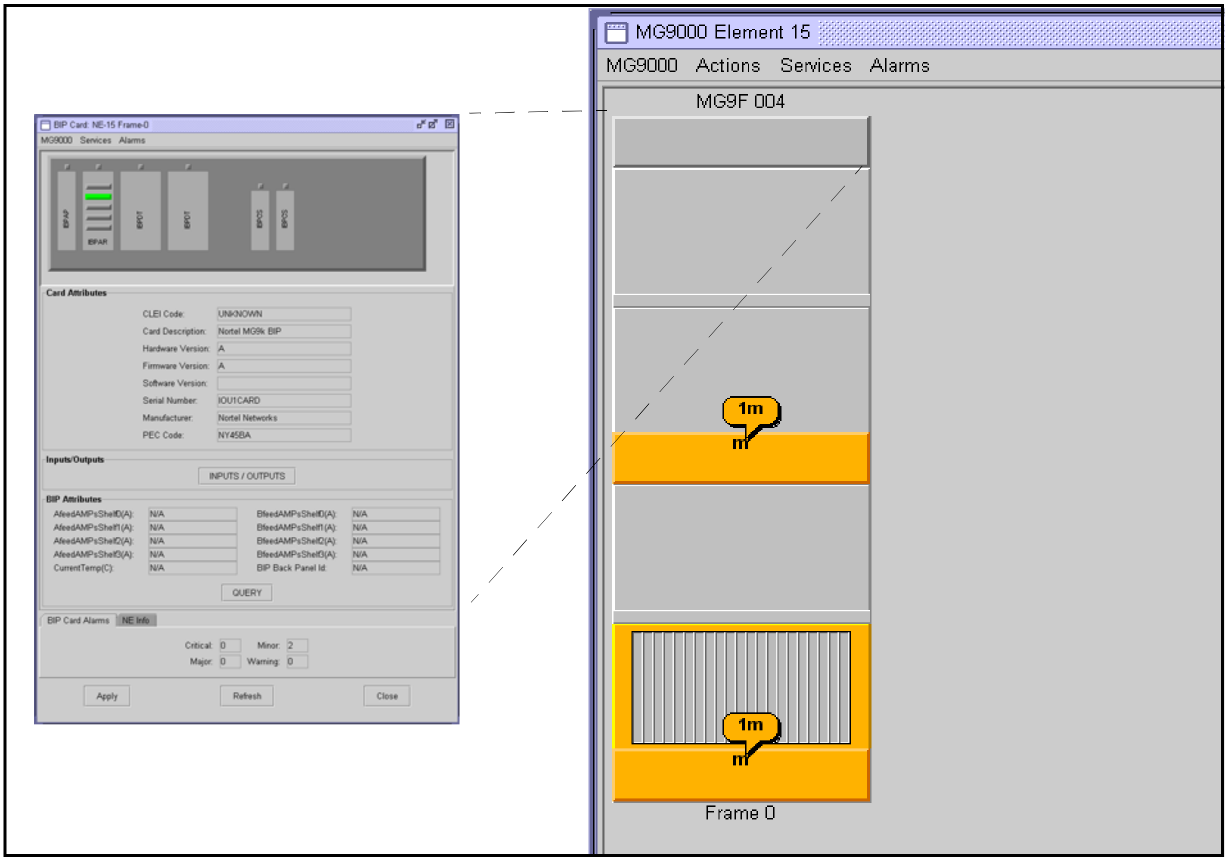
Viewing current frame-level alarms The frame alarm subsystem has a maximum of four links that connect the shelves to the BIP shelf. With these links, the shelves and the BIP shelf perform low-level non-mission critical communication. The BIP shelf receives the fan fail signals and lamp test/alarm cutoff (ACO) signal. The BIP reports the signals to the SIC card.

The BIP provides the following lamps on the front panel to indicate the alarm severity of the network elements in the frame:

- critical (red)
- major (red)
- minor (amber/yellow)

The following figure shows the Frame View and the IBIP Card View which is accessed by double-clicking on the IBIP within the Frame View.

Frame and IBIP card Views



CLEI Code: UNKNOWN
Card Description: Nortel MG9k BIP
Hardware Version: A
Firmware Version: A
Software Version:
Serial Number: IOU1CARD
Manufacturer: Nortel Networks
PEC Code: NY45BA

AfeedAMPsShelf0(A): N/A
AfeedAMPsShelf1(A): N/A
AfeedAMPsShelf2(A): N/A
AfeedAMPsShelf3(A): N/A
CurrentTemp(C): N/A
BfeedAMPsShelf0(A): N/A
BfeedAMPsShelf1(A): N/A
BfeedAMPsShelf2(A): N/A
BfeedAMPsShelf3(A): N/A
BIP Back Panel Id: N/A

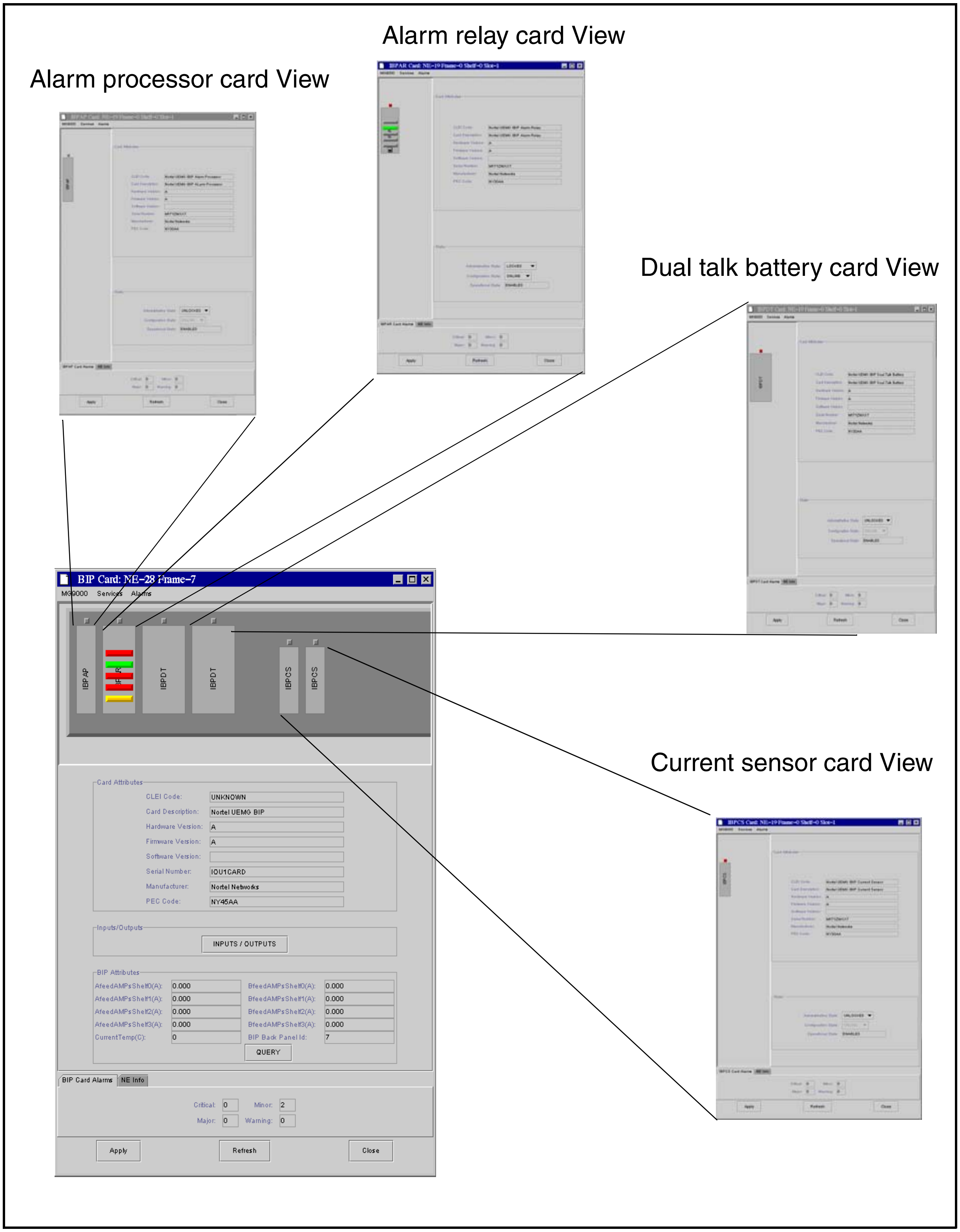
Critical: 0
Major: 0
Minor: 2
Warning: 0

The IBIP architecture has the IBIP as the main card and the following cards as sub-cards of this card:

- Alarm Processor card
- Alarm Relay card
- Dual Talk Battery card
- Current Sensor card

Each sub-card can be opened as a card view when the user double-clicks on the card. The Administrative and Configuration States of these cards can be set to enable replacement. The following figure shows the IBIP and sub-card views.

IBIP View and sub-card views



Alarm relay card View

Alarm processor card View

Dual talk battery card View

Current sensor card View

BIP Card: NE-28 Frame-7

Card Attributes

CLEI Code: UNKNOWN

Card Description: Nortel UEMG BIP

Hardware Version: A

Firmware Version: A

Software Version:

Serial Number: IOU1CARD

Manufacturer: Nortel Networks

PEC Code: NY45AA

Inputs/Outputs

BIP Attributes

AfeedAMPsShelf0(A):	0.000	BfeedAMPsShelf0(A):	0.000
AfeedAMPsShelf1(A):	0.000	BfeedAMPsShelf1(A):	0.000
AfeedAMPsShelf2(A):	0.000	BfeedAMPsShelf2(A):	0.000
AfeedAMPsShelf3(A):	0.000	BfeedAMPsShelf3(A):	0.000
CurrentTemp(C):	0	BIP Back Panel Id:	7

Critical: 0 Minor: 2

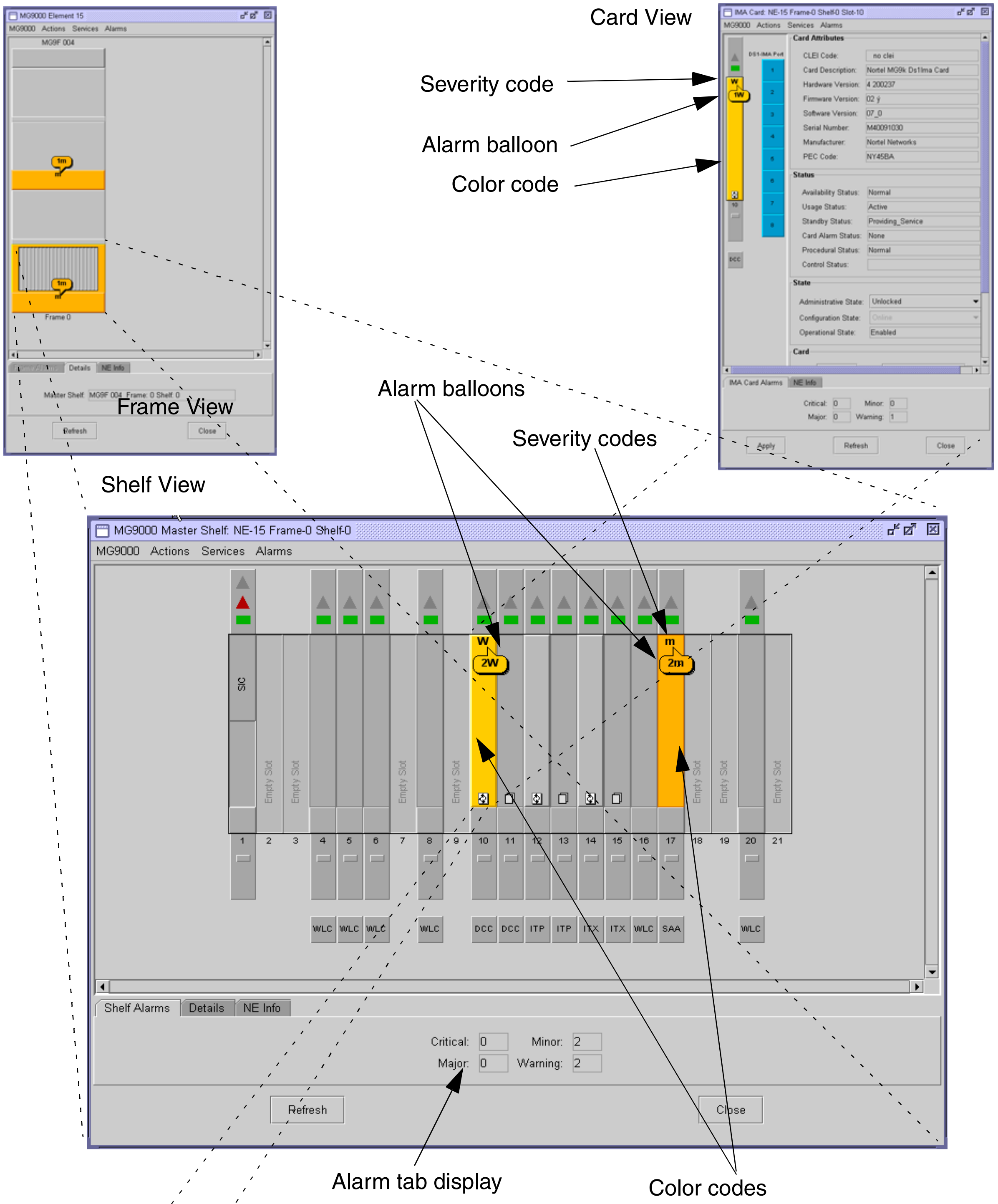
Major: 0 Warning: 0

Viewing shelf-level alarms The Shelf View which is accessed from the Frame View by double-clicking on the shelf, displays card alarm status through four different methods:

- color code
- alarm balloon
- severity code
- alarm tab

The following figure shows the Shelf View accessed from the Frame View and the shelf level alarms listed previously.

Frame, Shelf, and Card Views showing alarms



Master Shelf: MG9F 004 Frame: 0 Shelf: 0

Card Attributes

CLEI Code: no clei
Card Description: Nortel MG9k Ds1Ima Card
Hardware Version: 4 200237
Firmware Version: 02 ý
Software Version: 07_0
Serial Number: M40091030
Manufacturer: Nortel Networks
PEC Code: NY45BA

Status

Availability Status: Normal
Usage Status: Active
Standby Status: Providing_Service
Card Alarm Status: None
Procedural Status: Normal
Control Status:

State

Administrative State: Unlocked
Configuration State: Online
Operational State: Enabled

Card

Critical: 0 Minor: 0
Major: 0 Warning: 1

Critical: 0 Minor: 2
Major: 0 Warning: 2

For a list of the operational, state, and status icons used on the shelf and cards, see the MG 9000 alarm color codes table.

The colors follow the same pattern described in the following table and apply to both the cards and the alarm balloons.

MG 9000 alarm color codes

Alarm severity	Color	Explanation
Critical	Red	A critical alarm is raised when a severe, service-affecting condition requiring immediate action occurs.
Major	Red	A major alarm is raised for an event that meets one of the following definitions: • a serious disruption of service, or a malfunction of important circuits requiring immediate attention • conditions that may lead to a critical problem
Minor	Orange	A minor alarm is raised for an event that meets one of the following definitions: • problems that do not have a serious effect on service • circuit problems that are not required for call processing • conditions that may lead to major problems
Warning	Yellow	A warning alarm is raised for any problem that does not currently affect service and is not likely to become a serious service-affecting problem.

Severity codes are also used on the card and in the alarm balloons. The following table shows the Shelf View severity codes.

Shelf View and Card View Severity Codes

Code	Meaning
C	Critical
M	Major
m	Minor
W	Warning

Alarm balloons appear when new alarms occur. The balloons contain the severity code and provide additional alarm information listed in the following table.

Shelf View and Card View Alarm Balloon

Code	Explanation	Example	Meaning
<n><a>	The number of alarms, of that severity, for the card.	1C 2m	1 critical alarm 2 minor alarms
+	Alarms of lower severity also apply to that card.	1C+	One critical alarm exists, plus at least one major or minor alarm.

The Alarm tab display enumerates the number of alarms by severity code for the shelf being displayed.

Viewing circuit-level alarms The following line circuit cards offer additional indicators in the Card level view to show circuit-level alarms:

- World line card (WLC)
- Global line card (GLC)
- Digital subscriber line xDSL (Voice circuits only)
- Service Adapter Access (SAA)

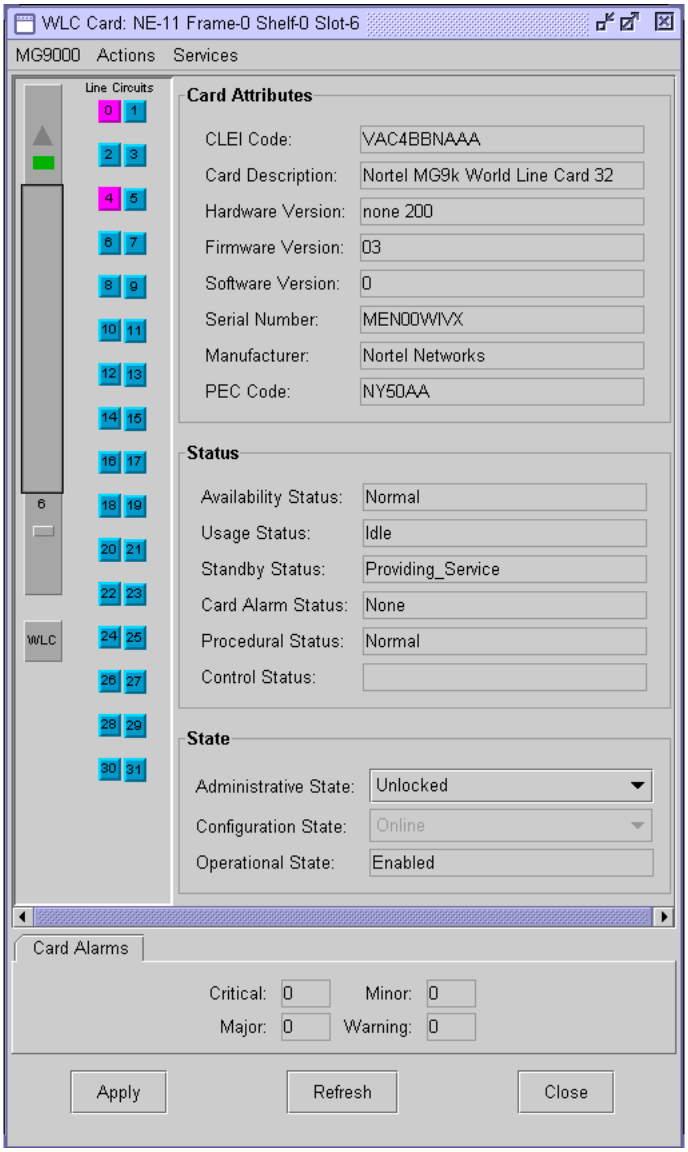
For further information about these line circuit cards, see *MG 9000 Configuration Management*, NN10096-511.

In normal operational state, circuits appear in blue. If a circuit is faulty it appears in magenta. If a circuit-level alarm occurs, the user can view the circuits that have alarms without opening a Circuit View. Alarm colors (red, orange, yellow) indicate the alarm severity.

> ***Note:*** The Faulty color indicator on a port takes precedence over Alarm indicators.

The figure WLC Card view showing faulty circuits displays the WLC Card view with circuit 0 and circuit 4 appearing in magenta indicating that they have been manually marked as faulty.

WLC Card view showing faulty circuits



Card Attributes

CLEI Code: VAC4BBNAAA

Card Description: Nortel MG9k World Line Card 32

Hardware Version: none 200

Firmware Version: 03

Software Version: 0

Serial Number: MEN00WIVX

Manufacturer: Nortel Networks

PEC Code: NY50AA

Status

Availability Status: Normal

Usage Status: Idle

Standby Status: Providing_Service

Card Alarm Status: None

Procedural Status: Normal

Control Status:

State

Administrative State: Unlocked

Configuration State: Online

Operational State: Enabled

Critical: 0 Minor: 0

Major: 0 Warning: 0

Audit NE alarms

The Audit alarms command is used to synchronize alarm data between the MG 9000 and the MG 9000 Manager and synchronizes alarms generated by the MG 9000 Manager.

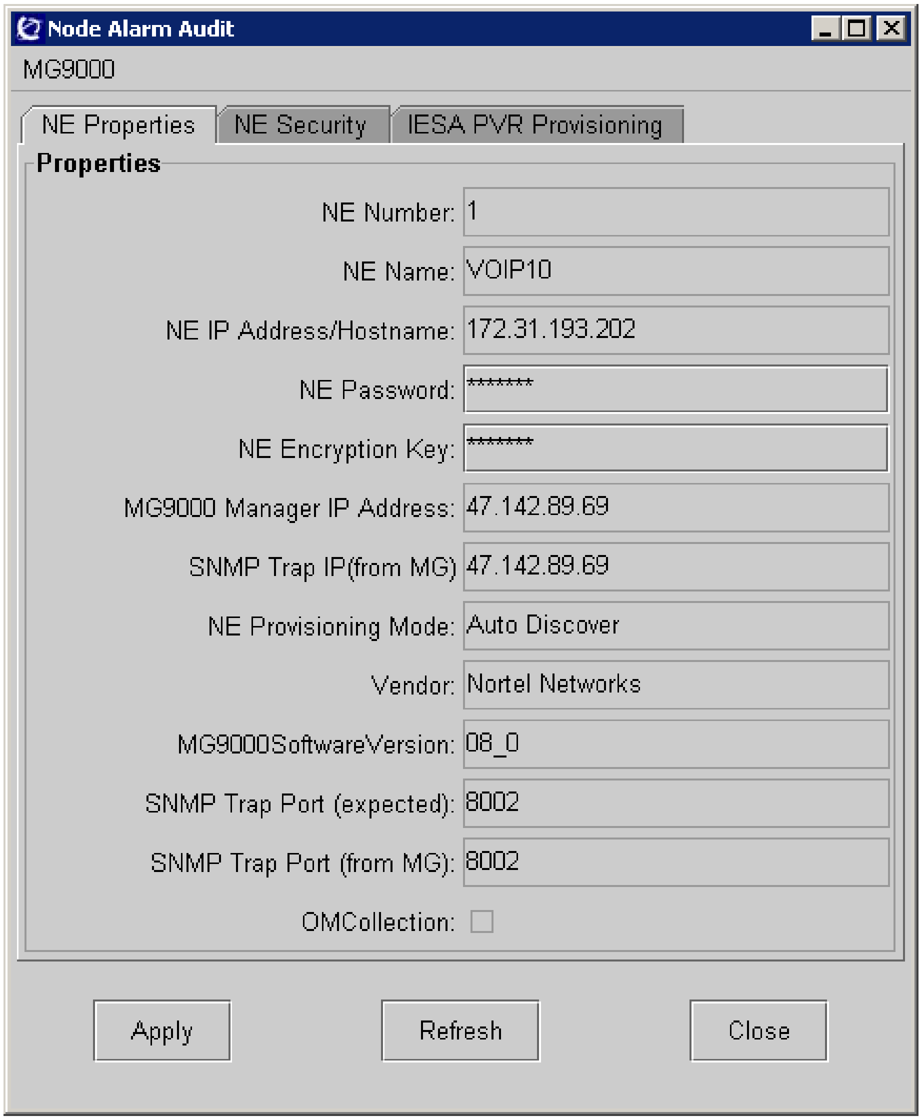
Synchronizing alarm data using Audit NE alarms

At the MG 9000 Manager

1 At the Subnet View, click on the MG 9000 NE on which the Audit alarm is to be performed. Alternately, access the NE desktop view for the selected NE.

2 From the menu bar, select Alarm->Audit NE alarms. The Node Alarm Audit view appears. The command can also be accessed from the NE desktop view for a specific NE. The following figure shows the Node Alarm Audit view.

Node Alarm Audit view



NE Number: 1

NE Name: VOIP10

NE IP Address/Hostname: 172.31.193.202

NE Password: *******

NE Encryption Key: *******

MG9000 Manager IP Address: 47.142.89.69

SNMP Trap IP(from MG) 47.142.89.69

NE Provisioning Mode: Auto Discover

Vendor: Nortel Networks

MG9000SoftwareVersion: 08_0

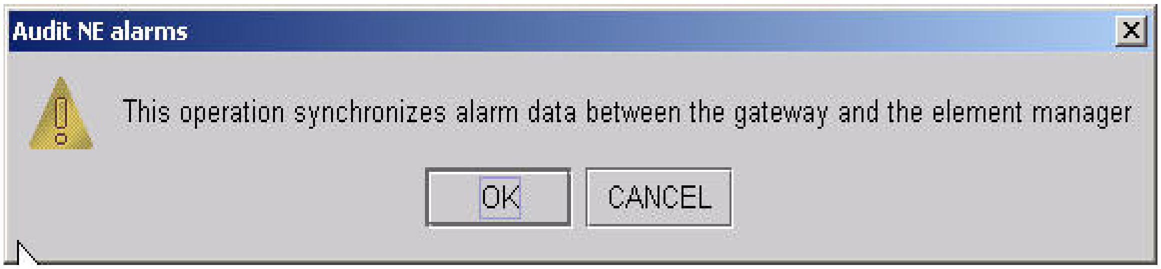
SNMP Trap Port (expected): 8002

SNMP Trap Port (from MG): 8002

OMCollection: □

3 Click Apply to initiate the Audit Alarms. The following message appears.

Audit node alarms message



Audit NE alarms

This operation synchronizes alarm data between the gateway and the element manager

4 Click OK to continue.

5 This procedure is complete.

Fault management procedures

Use the fault management information and procedures in this section to diagnose and clear faults in the MG 9000 and the MG 9000 Manager.

Retrieving MG 9000 alarms

Purpose of this procedure

This procedure provides access to service-related alarms on the MG 9000.

> ***Note:*** To all alarms for all MG 9000 network elements being served by the MG 9000 Manager, select Alarm->Alarm Browser from the menu at the top of the Subnet View. To view alarms by individual MG 9000 network element, select Alarms->Alarm Browser from the menu at the top of the Frame or Shelf View.

When to use this procedure

Use this procedure as a primary source of fault diagnostic information.

Prerequisites

This procedure has no prerequisites

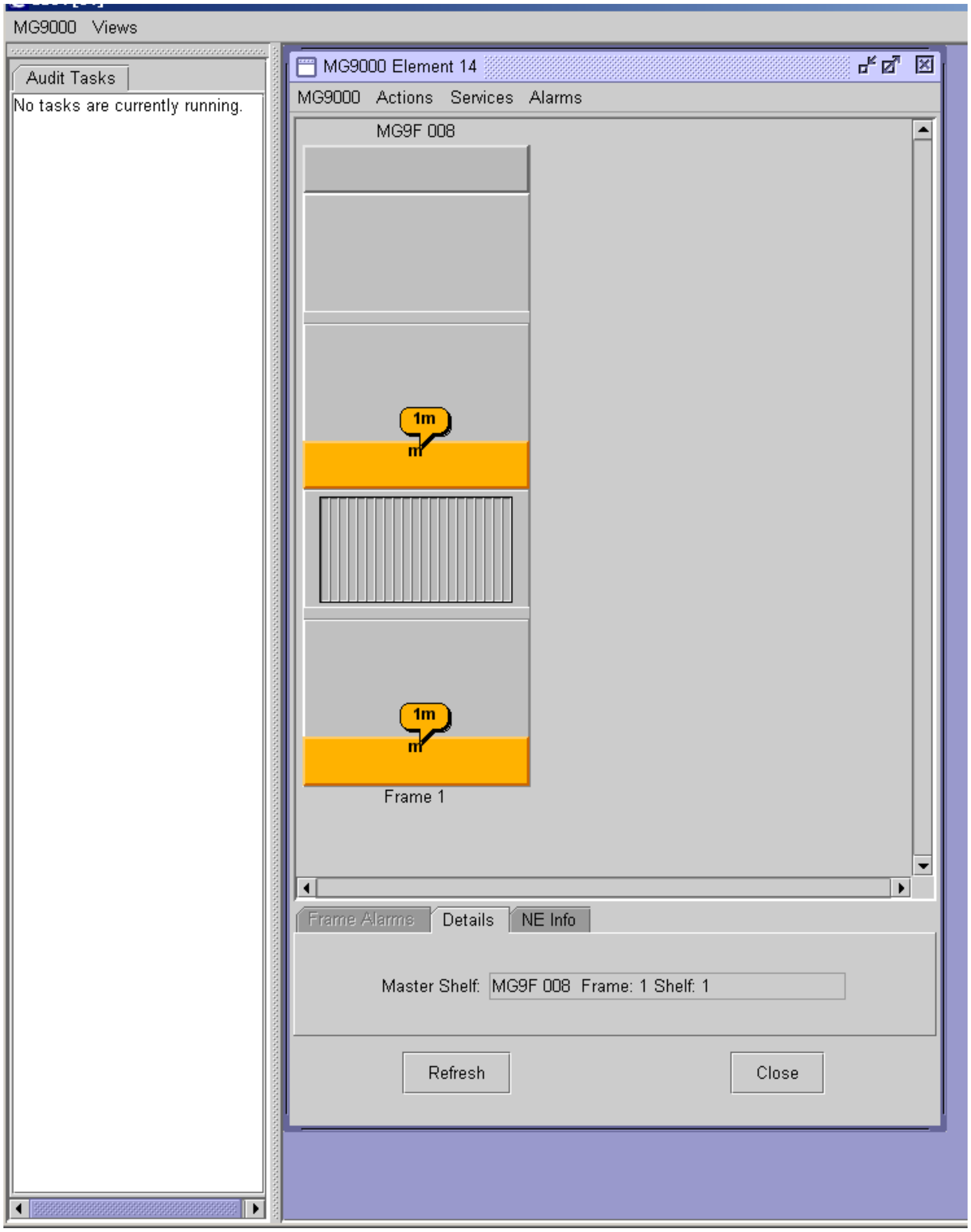
Action

Retrieving MG 9000 alarms

At the MG 9000 Manager

1 At the Subnet View, double-click on the MG 9000 icon in the tree view on the left or on the MG 9000 icon in the MG 9000 Manager view on the right, to select the MG 9000 for which alarm information is to be viewed. The network element (NE) desktop view with the Frame View opens as shown in the following figure.

MG 9000 Frame View within the NE desktop view



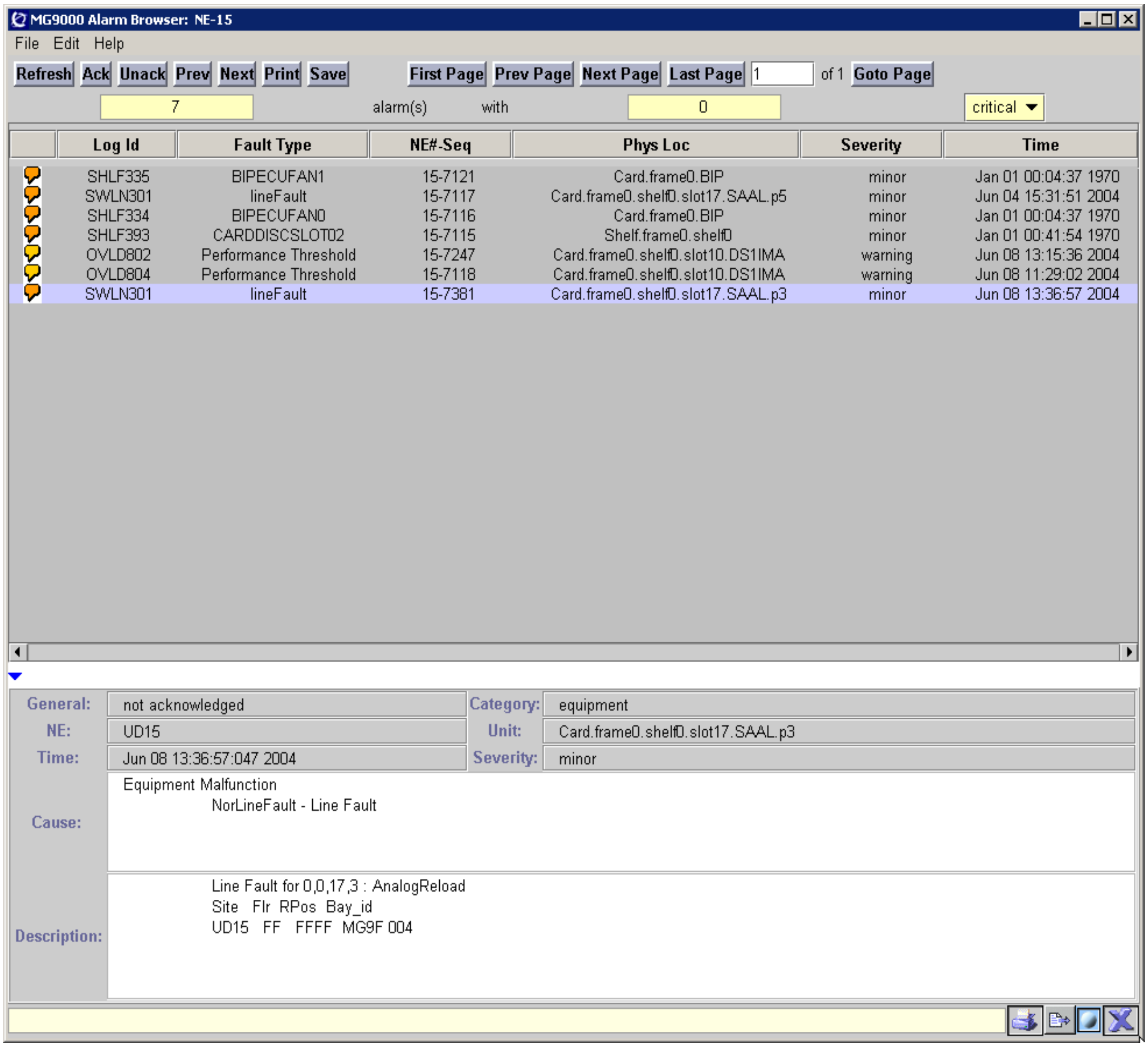
No tasks are currently running.

Master Shelf: MG9F 008 Frame: 1 Shelf: 1

2 At the top of the Frame View, select Alarm Browser from the Alarms menu at the top of the screen.

3 The Alarm Browser screen appears.

MG 9000 Alarm Browser showing alarms


MG9000 Alarm Browser: NE-15
File Edit Help
Refresh Ack Unack Prev Next Print Save
First Page Prev Page Next Page Last Page 1 of 1 Goto Page
7 alarm(s) with 0 critical

	Log Id	Fault Type	NE#-Seq	Phys Loc	Severity	Time
	SHLF335	BIPECUFAN1	15-7121	Card.frame0.BIP	minor	Jan 01 00:04:37 1970
	SWLN301	lineFault	15-7117	Card.frame0.shelf0.slot17.SAAL.p5	minor	Jun 04 15:31:51 2004
	SHLF334	BIPECUFAN0	15-7116	Card.frame0.BIP	minor	Jan 01 00:04:37 1970
	SHLF393	CARDDISCSLOT02	15-7115	Shelf.frame0.shelf0	minor	Jan 01 00:41:54 1970
	OVLD802	Performance Threshold	15-7247	Card.frame0.shelf0.slot10.DS1IMA	warning	Jun 08 13:15:36 2004
	OVLD804	Performance Threshold	15-7118	Card.frame0.shelf0.slot10.DS1IMA	warning	Jun 08 11:29:02 2004
	SWLN301	lineFault	15-7381	Card.frame0.shelf0.slot17.SAAL.p3	minor	Jun 08 13:36:57 2004

General: not acknowledged
Category: equipment
NE: UD15
Unit: Card.frame0.shelf0.slot17.SAAL.p3
Time: Jun 08 13:36:57:047 2004
Severity: minor

Cause:
Equipment Malfunction
NorLineFault - Line Fault

Description:
```
Line Fault for 0,0,17,3 : AnalogReload
Site  Flr  RPos  Bay_id
UD15  FF   FFFF  MG9F 004
```

4 Review the alarms in the Alarm Browser.

5 This procedure is complete.

Retrieving MG 9000 logs

Purpose of this procedure

This procedure provides access to log reports generated by the MG 9000 and transferred to the MG 9000 Manager.

All MG 9000 logs are written to the MG 9000 Manager. The MG 9000 Manager writes the logs into the following files:

- /var/log/customerlog (customer log file) on the server and mid-tier or directly from the CS 2000 Core Manager
- /data/mg9kem/logs/mg9kem.deslog (designer log file) on the server and mid-tier
- /var/log/auditlog (audit log file) on the server and mid-tier
- client logs are saved in a debug file in the Java Web Start Application Manager as described in the table below

The log files are named using the convention listed in the following table.

MG 9000 log file types and storage

Log	Description	Storage
customerlog	Customer log	Customer logs are directed to the custlog file on the server and mid-tier. Logs are routed to the CS 2000 Core Manager. Refer to the Routing customer logs to the CS 2000 Core Manager procedure.
deslog	Designer log	Designer logs are directed to the server and mid-tier.
auditlog	Audit log	Audit logs are directed to the server and mid-tier
MG 9000 Manager client application log	Client log	Client application logs are saved in a debug file available from the Java Web Start Application Manager. For steps to set up the debug file, refer to the “Saving MG 9000 Manager client application logs in a debug file” procedure in *MG 9000 Security and Administration*, NN10162-611

A standard text viewer is used for viewing logs sent to the MG 9000 Manager.

Log files constantly accumulate data and can eventually become difficult to manage and command large amounts of disk storage. Periodic log rotations keep the logs to a manageable size. The logs are rotated with the number 0 to 27 appended to the log file. Log files are compressed using gzip and will be appended with gz as shown in this example: mg9kem.deslog.0.gz. Log files customerlog and deslog are checked for rotation every 4 hours. If the log file size is over 1 Mb, it is rotated. Older files are named customerlog1, customerlog2, and so forth. Files that are 7 days old or more are automatically deleted.

> ***Note:*** Do not manually delete the active log files (that is, customerlog or deslog files). Log file rotation will not work properly if any of the active log files are missing. Log files can be retrieved manually and saved. Refer to the Retrieving MG 9000 logs procedure.

The following is an example of an MG 9000 log:

```
VMG 300 1723 TBL  MG9K NnMegacoFault
  Location: 1-RM9K-Frame000.Shelf2.Slot12
  Notification Id: 885
  State: not acknowledged
  Category: Equipment Alarm
  Cause: Equipment Malfunction
  Time: Apr 24 15:11:34 2003
  Component Id: Card.frame0.shelf2.slot12.ITP
  Specific Problem: NnMegacoFault - Root Termination Status    change
  Description: Call Processing Out of Service
```

The log report contains a log header line and the log body. The log event type appears in capital letters on the log header line. The following table shows the MG 9000 logs adaptor category types and log number ranges.

Logs adaptor log event types

Category	Range	Explanation
Trouble	300-399	Are the most important logs and indicate departures from normal operations.
Service Summary	400-499	Describe a sequence of events or all the events that occurred during a period.
State Change	500-599	Describe a change in state (for instance, from “in service” to “out of service”) of a specified entity.

Logs adaptor log event types

Category	Range	Explanation
Information	600-799	Used for problems detected by audits, corrective actions the system initiates, and system actions that do not require the technician to take action. Informational problems do not require corrective actions nor do they create alarms.
Threshold	800-899	Indicate that a number of similar events have exceeded a threshold value within a set period of time.
Expert	900-999	Internal log reports used by support personnel for debugging purposes. Expert logs are also known as extended or internal log reports.

MG 9000 logs

The logs seen at the MG 9000 Manager correlate to alarms seen at the Alarm Browser screen. In addition to the alarms being viewed at the MG 9000 Manager, alarms are also forwarded to the Operator Services System (OSS) for network level alarm monitoring.

To retrieve specific logs, use the logquery command at the CS2000 Core Manager. Refer to *CS2000 Core Manager Fault Management*, NN10082-911.

The logs output for the MG 9000 are listed in *Carrier VoIP Fault Management Logs Reference Manual*, NN10275-909.

If the log is reporting a problem with a card, an alarm will be displayed at the MG 9000 Manager. In the section that follow, the actual alarms raised against components are listed along with actions to be taken to clear the alarm.

When to use this procedure

Use this procedure as a part of scheduled maintenance and as a secondary source of diagnostic information.

Prerequisites

This procedure has no prerequisites.

Action

Retrieving MG 9000 logs

At the MG 9000 Manager

1 FTP to MG 9000 Manager server or mid-tier workstation.

2 Navigate to the directory where the custlog, deslog, or auditlog files are stored. Choose the log file to be viewed based on the possible date that the log was output.

> ***Note:*** The log files are appended with numbers 1 to 27, with the lower numbers being the newer files.

3 FTP a copy of the file into the working directory for viewing or save to the directory to prevent losing any log data from these files.

4 Open the text viewer or save the file.

5 This procedure is complete.

Determining available disk space for log files

At the MG 9000 Manager

1 To determine the space available for the log files, use the following Unix command.

```
> df -k /data/mg9kem/logs/
```

for designer logs

or

```
> df -k /var/log
```

for customer and audit logs

The output provides the current disk usage to determine if older files should be deleted.

2 This procedure is complete.

Routing customer logs to the CS 2000 Core Manager

At your workstation

1 Telnet to the MG 9000 Manager master server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the MG 9000 Manager master server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the Configuration option by typing

2

and pressing the Enter key.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - snmp_poller (SNMP Poller Configuration)
 X - exit

select -
```

7 Select the Syslog Configuration option by typing

8

and pressing the Enter key.

Example response

```
Syslog Configuration
 1 - list_syslog (List a system’s syslog
     configuration)
 2 - add_syslog (Add a syslog configuration
     entry)
 3 - del_syslog (Remove a syslog configuration
     entry)
 4 - route_syslog_on (Route syslog to the SDM)
 5 - route_syslog_off (Turn off syslog
     re-direction to SDM)

 X - exit

select -
```

8 Select the route_syslog_on option by typing

4

and pressing the Enter key.

Example response

```
=== Executing "route_syslog_on"
Available facilities are:
local1.notice
local7.notice
Please enter the facility to be routed:
```

9 Enter the facility to be routed by typing

`local1.notice`

```
Facility: local1.notice
Enter IP Address to route logs to :
```

10 Enter the IP Address used to send logs to /var/log/customerlog. This may be the SDM, CBM, or Integrated IEMS.

`<ip_address>`

where

<ip_address> is the address of the facility sending logs

```
47.xx.xxx.68 is alive
=== "route_syslog_on" completed successfully
```

11 Exit the command line interface by typing

x

and pressing the Enter key.

> ***Note:*** Exit each menu level to eventually exit the command line interface.

12 Syslog must be stopped and restarted for the change to take effect. To stop syslog, type

```
# /etc/init.d/syslog stop
```

13 To start syslog, type

```
# /etc/init.d/syslog start
```

14 You have completed this procedure.

Recovering an out-of-service MG 9000

Purpose of this procedure

Use this information to recover an out-of-service MG 9000.

The following are included in this section

- MG 9000 recovery flowchart
- Recovering an out-of-service MG 9000 that has not lost power and communicates with the MG 9000 Manager
- Recovering an MG 9000 that has lost power and cannot communicate with the MG 9000 Manager

When to use this procedure

Use these procedures in response to a loss of service by the MG 9000.

Prerequisites

An out-of-service MG 9000.

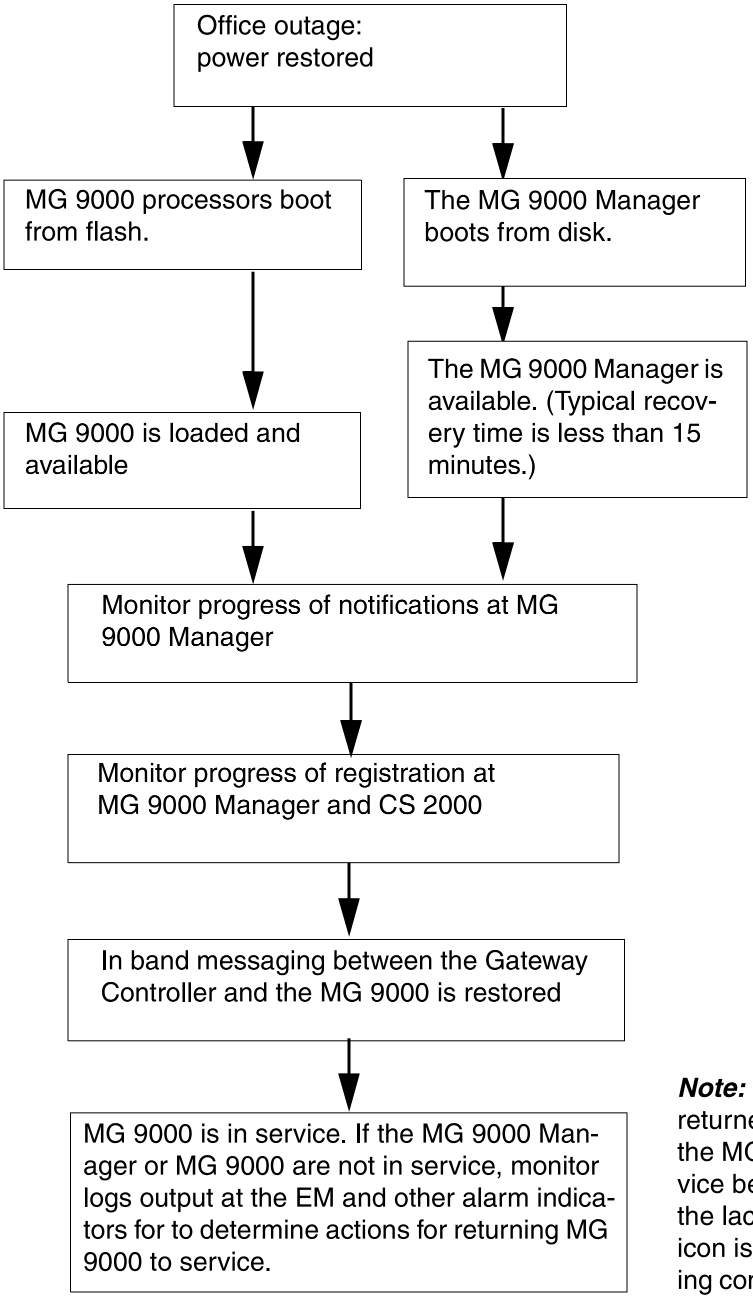
Action

If an MG 9000 is completely out of service, the MG 9000 will return to service autonomously once power is restored. The MG 9000, like other components in the Carrier VoIP solution are designed to recover autonomously without user intervention. Operating company personnel should monitor the progress to ensure that no additional faults prevent the MG 9000 from being restored. If the outage was the result of a loss of power, operating company personnel must restore power to begin recovery. There is no other requirement for user intervention at any of the phases of recovery.

The following flowchart identifies the activities the MG 9000 performs to recover from an outage and the activities operating company personnel observe during recovery.

MG 9000 recovery activities

MG 9000 Manager
and MG 9000 activities


Office outage: power restored
MG 9000 processors boot from flash.
The MG 9000 Manager boots from disk.
The MG 9000 Manager is available. (Typical recovery time is less than 15 minutes.)
MG 9000 is loaded and available
Monitor progress of notifications at MG 9000 Manager
Monitor progress of registration at MG 9000 Manager and CS 2000
In band messaging between the Gateway Controller and the MG 9000 is restored
MG 9000 is in service. If the MG 9000 Manager or MG 9000 are not in service, monitor logs output at the EM and other alarm indicators for to determine actions for returning MG 9000 to service.

Activities operating company personnel observe.

Monitor captive office LAN status at Multiservice Switch 8600. Check the individual status of captive office LAN connected equipment at the MG 9000 Manager displays. There will be no communication until the Multiservice Switch 8600s are up.

Because of the possibility that a transmission multiplexer is present, the OC-3 carrier at the MG 9000 or Multiservice Switch15000 do not indicate that an OC-3 carrier is established.

MG 9000 sends a cold start to the MG 9000 Manager

After the GWC is in service, the MG 9000 informs the MG 9000 Manager that the VMGs are in service.

Lines are scanning for off hook.

MG 9000 discovery in process.

Note: Determine if the MG 9000 Manager returned to service before the MG 9000. If the MG 9000 Manager did not return to service before the MG 9000, as evidenced by the lack of NE icons or the not discovered icon is present above the NE icon, operating company personnel will have to perform a manual discovery at the MG 9000 Manager.

Recovering an out-of-service MG 9000 that has not lost power and communicates with the MG 9000 Manager

Use the following procedure when the MG 9000 is out-of-service yet communication with the MG 9000 Manager is available.

> ***Note 1:*** The following procedures are intended for use when the previous methods to return an out-of-service MG 9000 to service are unsuccessful.
>
> ***Note 2:*** Before proceeding with the following procedure, it is recommended that Nortel Networks be contacted for technical assistance.

Recovering an out-of-service MG 9000 that has not lost power and communicates with the MG 9000 Manager

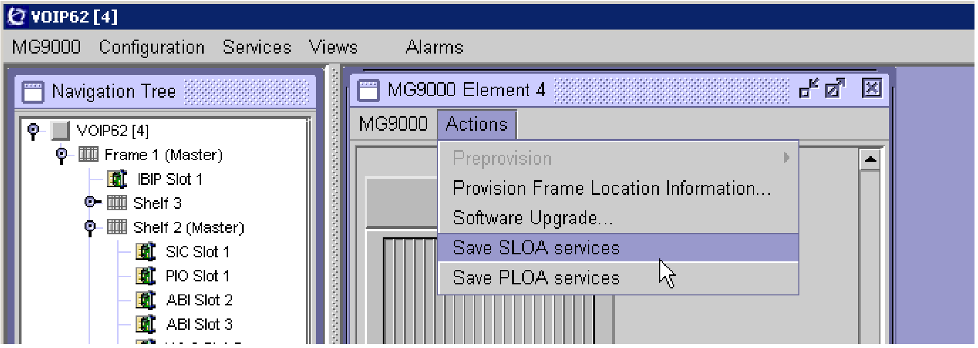
At the MG 9000 Manager

1 At the Subnet View of the MG 9000 Manager, double-click on the MG 9000 to be re-commissioned.

A warning window indicating that your connection to the gateway is down may appear. This will not block the saving of services information.

2 Save a copy of the MG 9000 Manager SLoA service provisioning data. At the Frame (Element) view, select Actions --> Save SLOA services option from the menu bar.

NE desktop view with Frame View

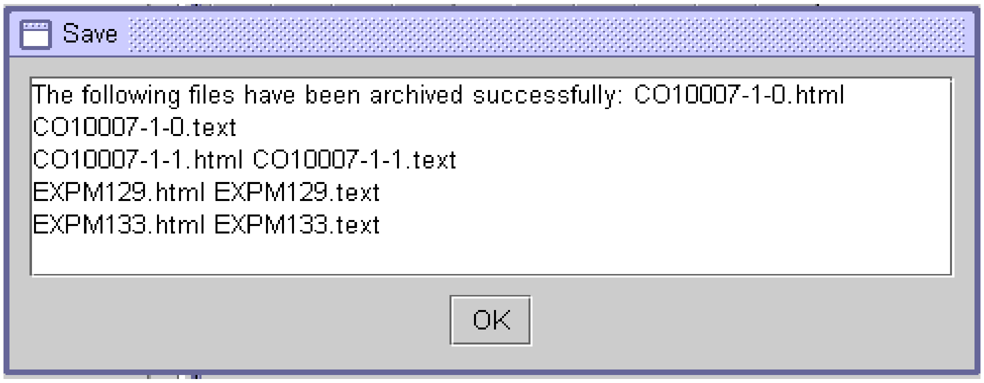


An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the two files (with .html and .text suffixes) where the data was stored on the MG 9000 Manager.

3 Record the file name provided in the Save acknowledgement window for later use.

The following figure shows an example of the Save acknowledgement message. Your file names will depend on your network configuration.

Example of a Save acknowledgement message for SLoA



The following files have been archived successfully: CO10007-1-0.html
CO10007-1-0.text
CO10007-1-1.html CO10007-1-1.text
EXPM129.html EXPM129.text
EXPM133.html EXPM133.text

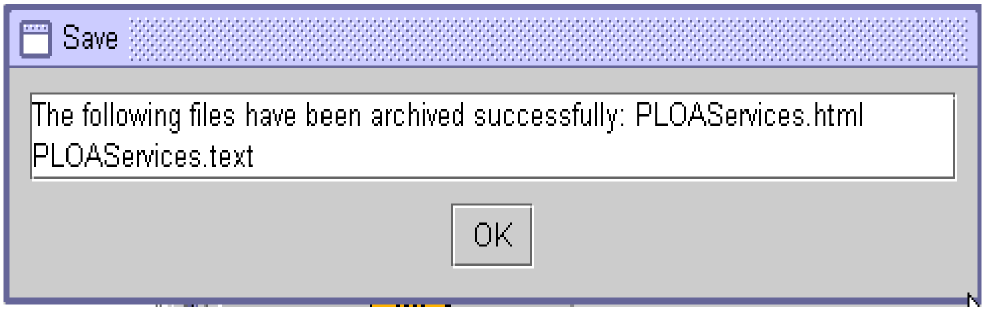
4 Save a copy of the MG 9000 Manager PLoA provisioning data. To save the PLoA services provisioning data, at the Frame (Element) view, select the “Save PLOA services” option from the Actions menu

An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the files where your data had been stored on the MG 9000 Manager.

5 Record the file name provided in the Save acknowledgement window for later use.

The following figure shows an example of the Save acknowledgement message. Your file names will depend on your network configuration.

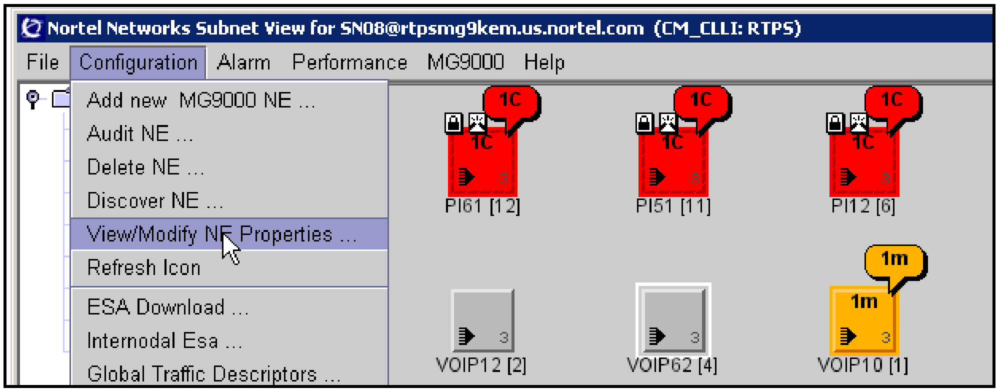
Example of a Save acknowledgement message for PLoA



The following files have been archived successfully: PLOAServices.html
PLOAServices.text

6 Obtain the IP address of the MG 9000 Manager server (not the mid-tier or client). At the Subnet View, select Configuration->View/Modify NE Properties from the menu bar.

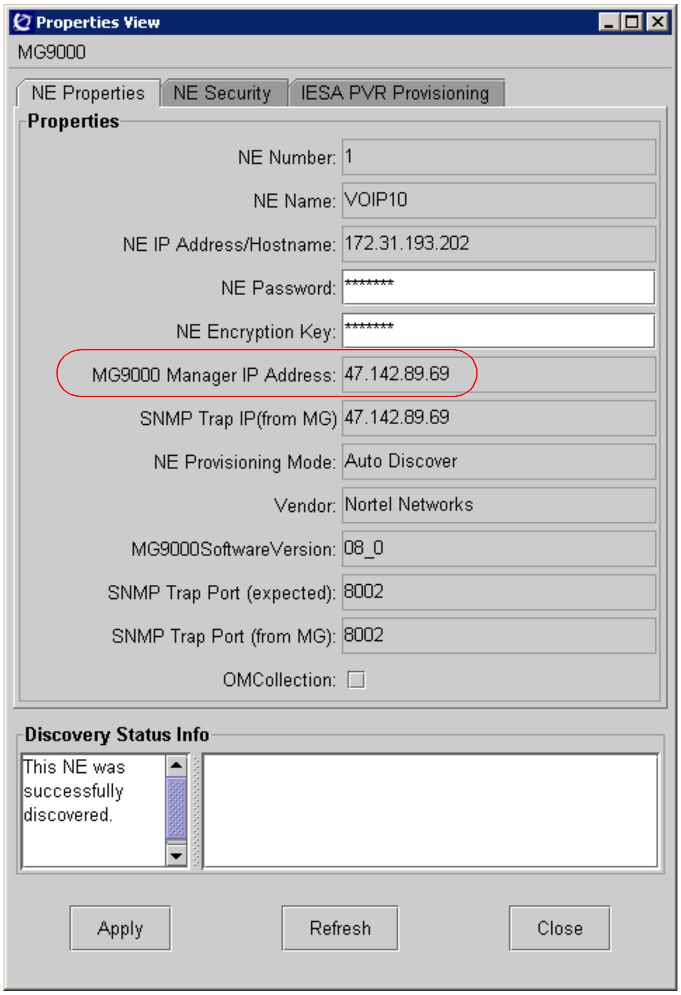
Subnet View accessing Configuration ->View/Modify NE Properties



7 Record the IP address in the MG 9000 Manager IP Address field.

The following figure shows the location of the IP address data (circled in red). The address in the figure is intended as an example; your data depends on your network configuration.

Properties View: an example showing the location of IP Address field



MG9000

Properties

NE Number:	1
NE Name:	VOIP10
NE IP Address/Hostname:	172.31.193.202
NE Password:	*******
NE Encryption Key:	*******
MG9000 Manager IP Address:	47.142.89.69
SNMP Trap IP(from MG)	47.142.89.69
NE Provisioning Mode:	Auto Discover
Vendor:	Nortel Networks
MG9000SoftwareVersion:	08_0
SNMP Trap Port (expected):	8002
SNMP Trap Port (from MG):	8002
OMCollection:	□

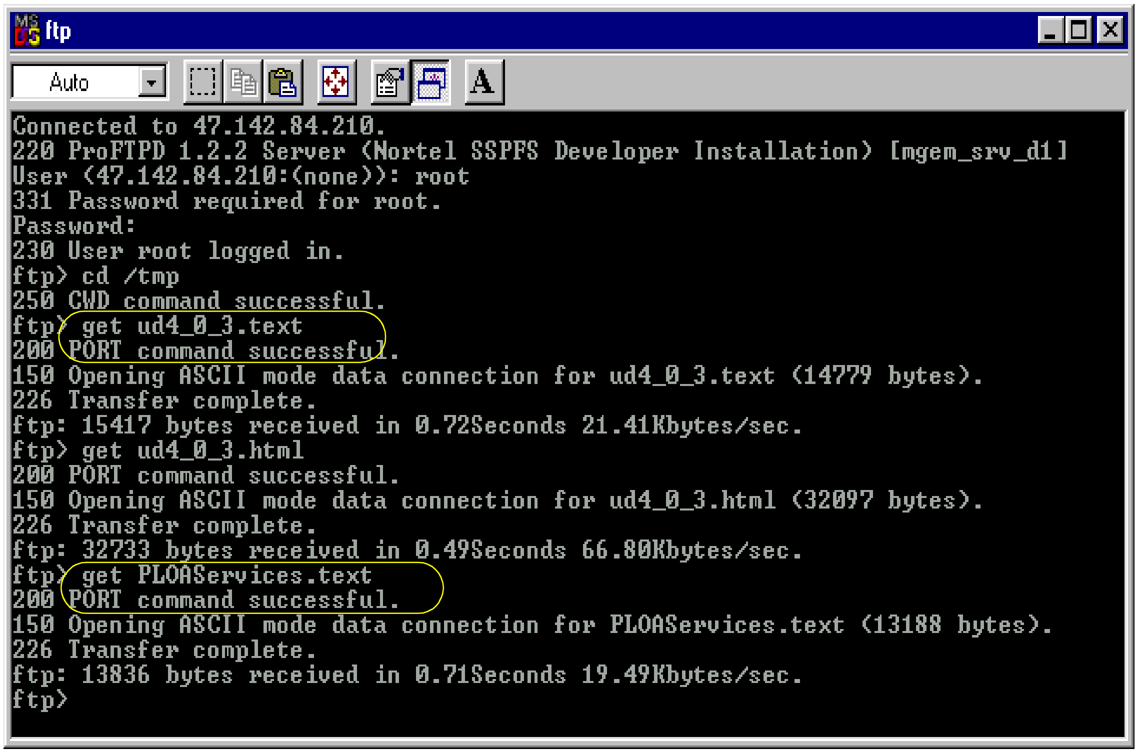
Discovery Status Info

This NE was successfully discovered.

8 FTP to the address recorded in Step 7.

9 Using the file names that you recorded in Steps 3 and 5, copy the files in the /tmp directory to a secure location, such as your desktop or permanent server before proceeding.

FTP session: an example of a file transfer to a secure location



```
Connected to 47.142.84.210.
220 ProFTPD 1.2.2 Server (Nortel SSPFS Developer Installation) [mgem_srv_d1]
User (47.142.84.210:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> get ud4_0_3.text
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.text (14779 bytes).
226 Transfer complete.
ftp: 15417 bytes received in 0.72Seconds 21.41Kbytes/sec.
ftp> get ud4_0_3.html
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.html (32097 bytes).
226 Transfer complete.
ftp: 32733 bytes received in 0.49Seconds 66.80Kbytes/sec.
ftp> get PLOAServices.text
200 PORT command successful.
150 Opening ASCII mode data connection for PLOAServices.text (13188 bytes).
226 Transfer complete.
ftp: 13836 bytes received in 0.71Seconds 19.49Kbytes/sec.
ftp>
```

10 To clear persistence on the MG 9000.

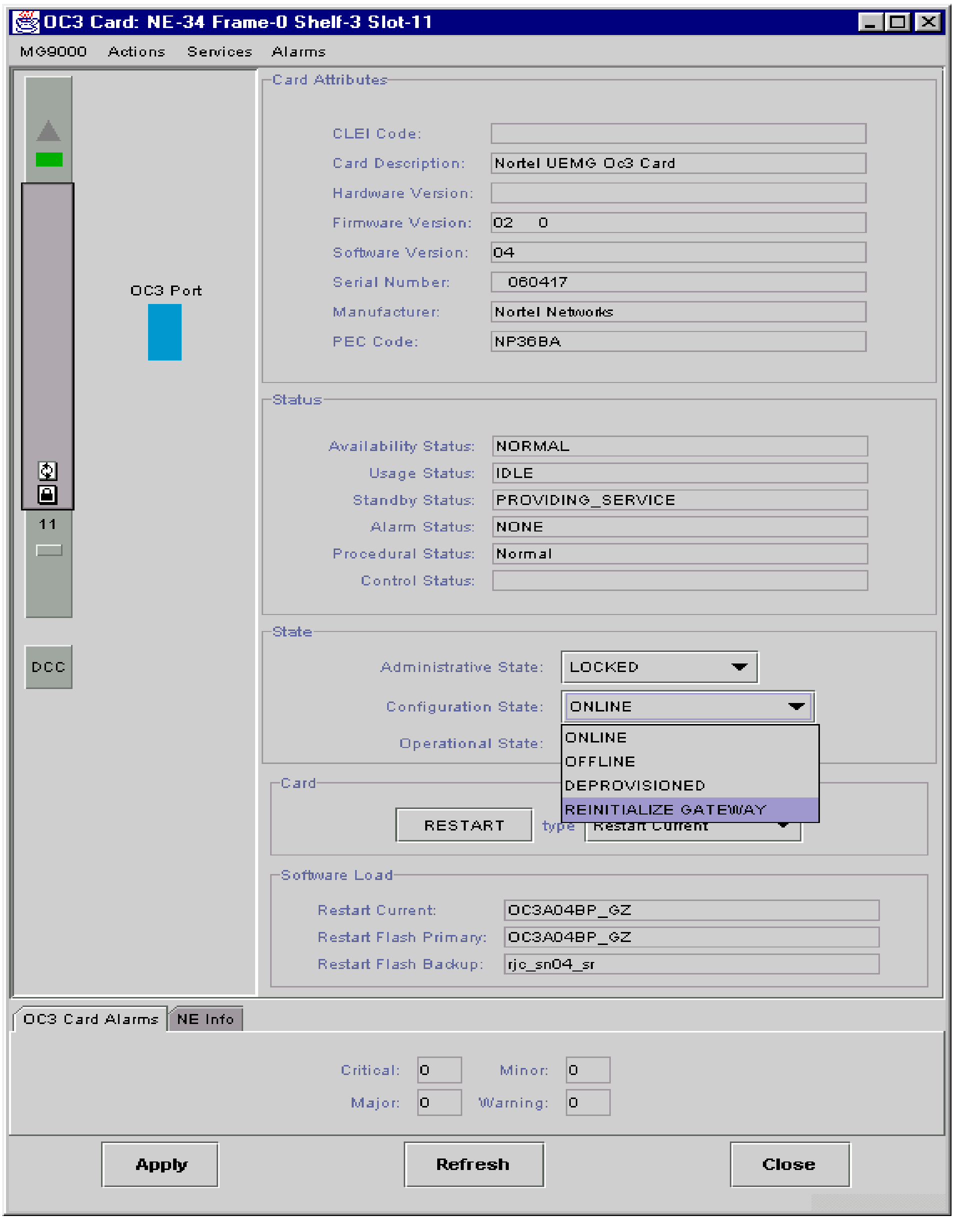
a From the Frame View, double click on the master shelf. The Shelf View appears.

b From the Shelf View, double click on the inactive OC-3 or DS1 IMA card. The OC-3/IMA Card View appears.

c At the OC-3/DS1 IMA Card View, set the Administrative State of the inactive card to Forced Lock. Then set the Configuration State to offline. After the inactive card is locked and set to offline, then repeat these steps for the active OC-3/DS1 IMA card.

d From the OC-3/DS1 IMA Card View, from the Configuration State pull-down menu, select Reinitialize Gateway as shown in the following figure.

OC-3 Card View



OC3 Card: NE-34 Frame-0 Shelf-3 Slot-11

Card Attributes

CLEI Code:
Card Description: Nortel UEMG Oc3 Card
Hardware Version:
Firmware Version: 02 0
Software Version: 04
Serial Number: 060417
Manufacturer: Nortel Networks
PEC Code: NP36BA

Status

Availability Status: NORMAL
Usage Status: IDLE
Standby Status: PROVIDING_SERVICE
Alarm Status: NONE
Procedural Status: Normal
Control Status:

State

Administrative State: LOCKED
Configuration State: ONLINE
Operational State:

ONLINE
OFFLINE
DEPROVISIONED
REINITIALIZE GATEWAY

Card

RESTART type Restart Current

Software Load

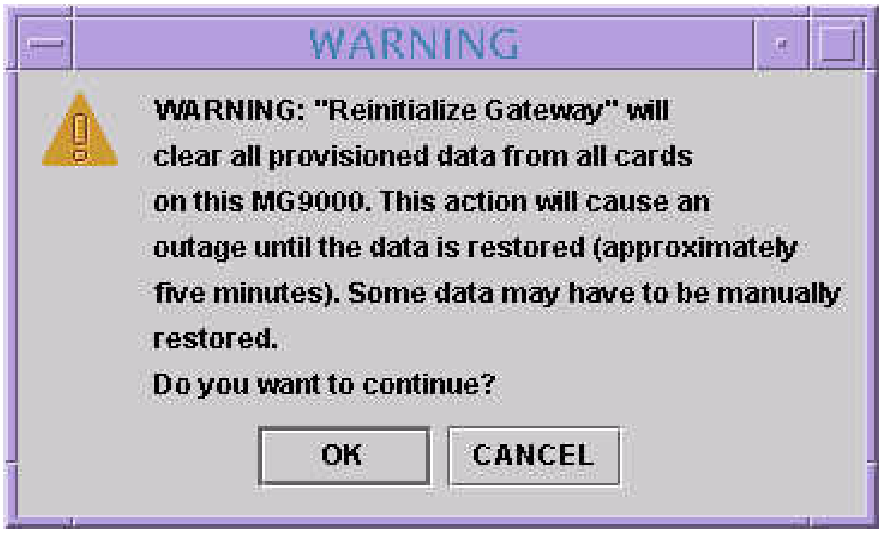
Restart Current: OC3A04BP_GZ
Restart Flash Primary: OC3A04BP_GZ
Restart Flash Backup: rjc_sn04_sr

OC3 Card Alarms | NE Info

Critical: 0 Minor: 0
Major: 0 Warning: 0

e After setting the configuration state to “Reinitialize gateway”, a warning message appears requesting a reply before continuing. Select OK.

Warning message in response to Reinitialize Gateway



WARNING: "Reinitialize Gateway" will clear all provisioned data from all cards on this MG9000. This action will cause an outage until the data is restored (approximately five minutes). Some data may have to be manually restored.

Do you want to continue?

f The MG 9000 will restart, and the maintenance link to the MG 9000 Manager will drop.

Wait for the restart to complete, typically takes 5 minutes.

11 From the Frame View, double click on the master shelf. The Shelf View appears.

12 From the Shelf View, double click on the active OC-3 card. The OC-3 Card View appears.

13 At the OC-3 Card View, set the Configuration State to Online. Wait for the restart to complete. Set the Administrative State to Unlock. After the active card is Online, repeat this step for the inactive OC-3 card.

14 Provision the PLoA and SLoA services using the recovery files that were stored in step 8 and the Provisioning PLoA services and Provisioning SLoA services procedures in *MG 9000 Configuration Management*, NN10096-511.

15 Wait for the network element to show it is operational, then check for dial tone.

16 This procedure is complete.

Recovering an MG 9000 that has lost power and cannot communicate with the MG 9000 Manager

Use the following procedure when communication with the MG 9000 Manager is not available and power to the MG 9000 was lost.

> ***Note:*** Before proceeding with the following procedure, it is recommended that Nortel Networks be contacted for technical assistance.

Recovering an MG 9000 that has lost power and cannot communicate with the MG 9000 Manager

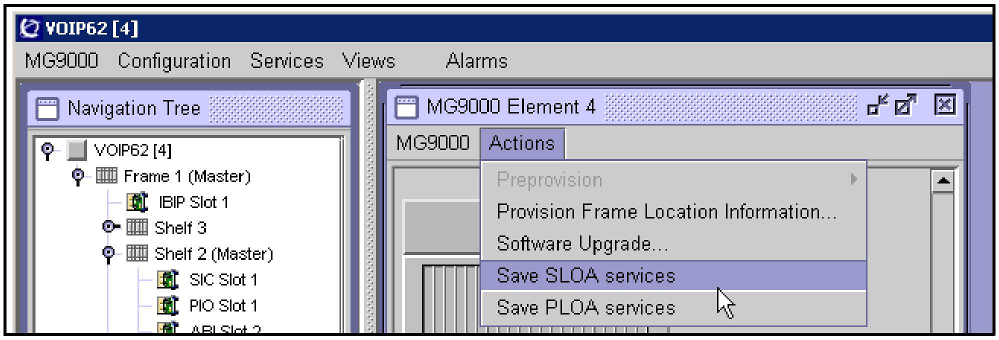
At the MG 9000 Manager

1 At the Subnet View of the MG 9000 Manager, select the MG 9000 to be re-commissioned.

A warning window indicating that your connection to the gateway is inoperative may appear. This will not block the saving of services information.

2 Save a copy of the MG 9000 Manager SLoA provisioning data. To Save the SLoA services provisioning data, at the Frame (Element) view, select the "Save SLOA services" option from the Actions menu.

NE desktop view with Frame View

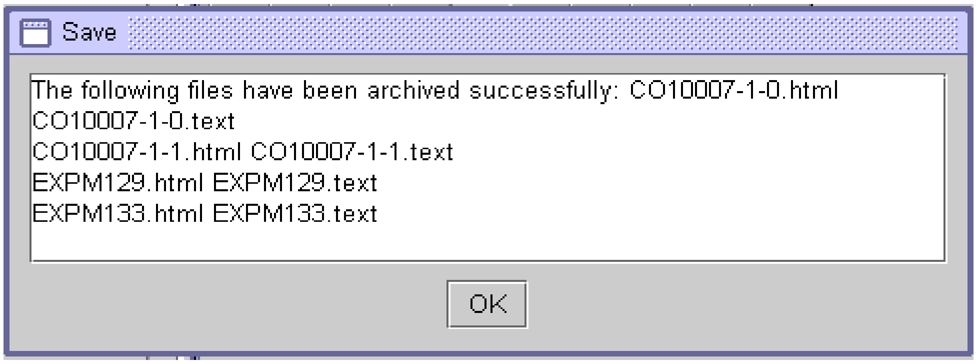


An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the two files (with .html and .text suffixes) where your data had been stored on the MG 9000 Manager.

3 Record the file name provided in the Save acknowledgement window for later use. You will re-enter this data later in this procedure.

The following figure shows an example of the Save acknowledgement message. Your file names will depend on your network configuration.

Example of a Save acknowledgement message for SLoA



The following files have been archived successfully: CO10007-1-0.html
CO10007-1-0.text
CO10007-1-1.html CO10007-1-1.text
EXPM129.html EXPM129.text
EXPM133.html EXPM133.text

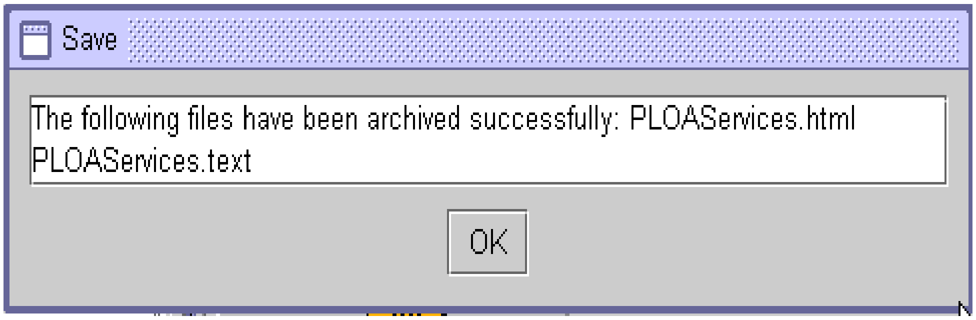
4 Save a copy of the MG 9000 Manager PLoA provisioning data. To save the PLoA services provisioning data, at the Frame (Element) view, select the “Save PLOA services” option from the Actions menu.

An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the files where your data had been stored on the MG 9000 Manager.

5 Record the file name provided in the Save acknowledgement window for later use. You will re-enter this data later in this procedure.

The following figure shows an example of the Save acknowledgement message. Your file names will depend on your network configuration.

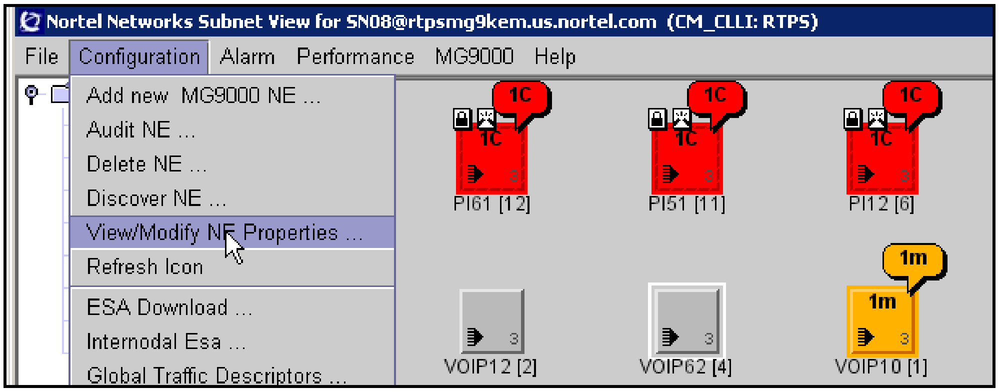
Example of a Save acknowledgement message for PLoA



The following files have been archived successfully: PLOAServices.html
PLOAServices.text

6 Obtain the IP address of the MG 9000 Manager server (not the mid-tier or client). At the Subnet View, select Configuration->View/Modify NE Properties from the menu bar.

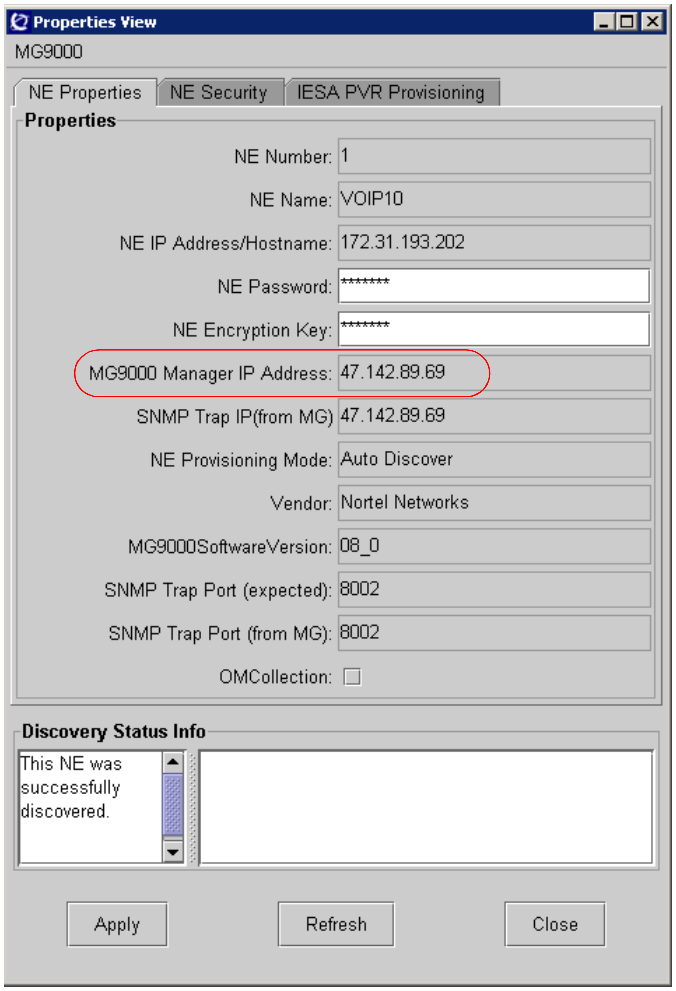
Subnet View accessing Configuration ->View/Modify NE Properties



7 Record the IP address in the MG 9000 Manager IP Address field. You will re-enter this data later in this procedure.

The following figure shows the location of the IP address data (circled in red). The address in the figure is intended as an example; your data depends on your network configuration.

Properties View: an example showing the location of IP Address field



NE Number: 1
NE Name: VOIP10
NE IP Address/Hostname: 172.31.193.202
NE Password: ********
NE Encryption Key: ********
MG9000 Manager IP Address: 47.142.89.69
SNMP Trap IP(from MG) 47.142.89.69
NE Provisioning Mode: Auto Discover
Vendor: Nortel Networks
MG9000SoftwareVersion: 08_0
SNMP Trap Port (expected): 8002
SNMP Trap Port (from MG): 8002
OMCollection: □

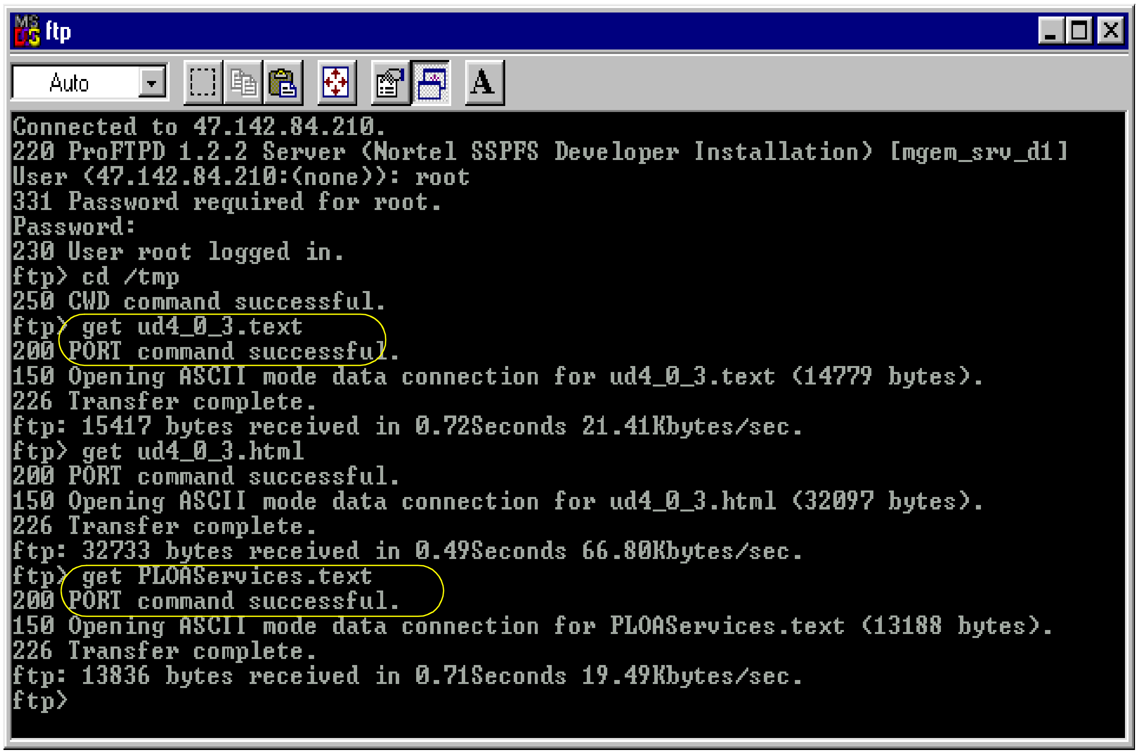
This NE was successfully discovered.

8 FTP to the address recorded in step 7.

9 Using the file names that you recorded in Steps 3 and 5, copy the files in the /tmp directory to a secure location, such as your desktop or permanent server before proceeding.

The following figure shows an example of an FTP session. The VMG files have the following format: <VMG name>.txt, where the VMG name is that assigned by your network administrator.

FTP session: an example of a file transfer to a secure location



```
Connected to 47.142.84.210.
220 ProFTPD 1.2.2 Server (Nortel SSPFS Developer Installation) [mgem_srv_d1]
User (47.142.84.210:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> get ud4_0_3.text
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.text (14779 bytes).
226 Transfer complete.
ftp: 15417 bytes received in 0.72Seconds 21.41Kbytes/sec.
ftp> get ud4_0_3.html
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.html (32097 bytes).
226 Transfer complete.
ftp: 32733 bytes received in 0.49Seconds 66.80Kbytes/sec.
ftp> get PLOAServices.text
200 PORT command successful.
150 Opening ASCII mode data connection for PLOAServices.text (13188 bytes).
226 Transfer complete.
ftp: 13836 bytes received in 0.71Seconds 19.49Kbytes/sec.
ftp>
```

At the MG 9000 frame

10 Remove power to the shelves by removing the fuse modules on the IBIP that provide power to the shelves.

At the MG 9000 frame

11 Power up the shelves in the frame by reinstalling the fuse modules on the IBIP that were removed in step 10.

12 Connect a laptop PC to the active DCC card and launch the local craft interface (LCI).

13 Wait for the restart to complete and for all cards to initialize, This step typically takes 5 minutes. The Administrative State of all common cards is Locked during this step.

14 From the LCI, Unlock the active DCC OC-3/DS1 IMA/GigE card by selecting the Admin. State Unlock radio button. Wait for the status at the LCI to change to Enabled, Online, and Unlocked.

15 From the LCI continue to unlock the common cards in the following order until all are unlocked and online:

- active ITX
- active ITP
- OC-3 carriers on the active OC-3 DCC card or GigE link on the active GigE DCC card
- inactive DCC
- inactive ITX
- inactive ITP
- OC-3 carriers on the inactive OC-3 DCC card or GigE link on the inactive GigE DCC card
- DS1 cards (if provisioned)
- ABI cards (if provisioned)

16 From the LCI, open the Connections tab, select OAMP connection, then select Reset Comm.

At the MG 9000 Manager

17 Monitor the MG 9000 network element and wait until the discovery process is complete.

18 Wait for the network element to show it is operational, then check for dial tone.

19 This procedure is complete.

Reinitialize gateway command

Purpose of this procedure

Use this information to reinitialize an MG 9000 network element.

The Reinitialize Gateway functionality allows the technician to clear persistent data and restart the MG 9000 from the MG 9000 Manager.

> ***Note 1:*** The Reinitialize Gateway functionality is only supported as part of an MG 9000 recovery scenario.
>
> ***Note 2:*** If the MG 9000 requires initialization due to corruption (persistence data clear for all intelligent cards), initiate the Reinitialize Gateway command from OC3/DS1 IMA/GigE Card View to clear MG 9000 persistence data. When this command is sent, the MG 9000 will clear all of its persisted data and go through re-discovery of all hardware. Once this discovery is completed, it will send a Cold Start trap to MG 9000 Manager. The MG 9000 Manager will retrieve all hardware-related information and then start audit and recovery. As a part of audit and recovery, the MG 9000 Manager will try to restore all configuration data at the MG 9000.

When to use this procedure

Use these procedures in response to a loss of service by the MG 9000.

Prerequisites

There are no prerequisites.

Action

Reinitialize the MG 9000 functionality

At the MG 9000 Manager

1

> **DANGER**
> **Do not initiate any actions using open GUIs until discovery of the MG 9000 network element is complete.**
> When using the Reinitialize gateway command, if any GUIs are open, do not initiate any maintenance actions on those GUIs other than to close them. Only initiate maintenance actions after discovery of the MG 9000 network element is complete.

At the Subnet View, double click on the MG 9000 icon that is to be reinitialized. The Frame View within the NE desktop view appears.

2 From the Frame View, double click on the master shelf. The Shelf View appears.

3 From the Shelf View, double click on the inactive OC-3/DS1 IMA/GigE card. The OC-3/DS1 IMA/GigE Card View appears.

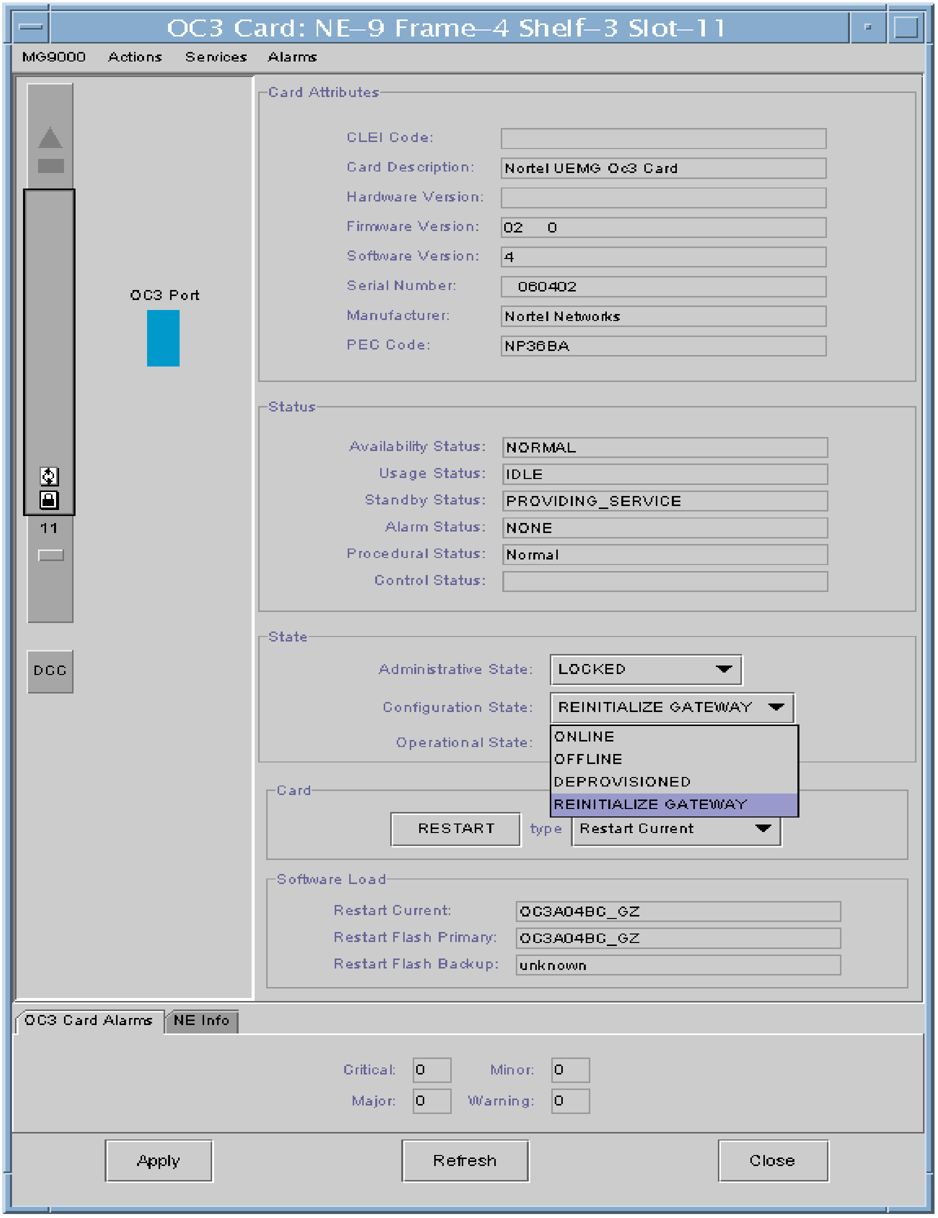
4 Set the Administrative State of the Inactive OC-3/DS1 IMA/GigE card to Forced Locked and respond to the message.

5 From the Shelf View, double click on the active OC-3/DS1 IMA/GigE card. The OC-3/DS1 IMA/GigE Card View appears.

6 Set the Administrative State of the active OC-3/DS1 IMA/GigE card to Forced Locked and respond to the message.

7 In the OC-3/DS1 IMA/GigE Card View, from the Configuration State pull-down menu, select Reinitialize Gateway as shown in the following figure.

OC-3 Card View



OC3 Card: NE–9 Frame–4 Shelf–3 Slot–11

Card Attributes

CLEI Code:	
Card Description:	Nortel UEMG Oc3 Card
Hardware Version:	
Firmware Version:	02 0
Software Version:	4
Serial Number:	060402
Manufacturer:	Nortel Networks
PEC Code:	NP36BA

Status

Availability Status:	NORMAL
Usage Status:	IDLE
Standby Status:	PROVIDING_SERVICE
Alarm Status:	NONE
Procedural Status:	Normal
Control Status:	

State

Administrative State:	LOCKED
Configuration State:	REINITIALIZE GATEWAY
Operational State:	

ONLINE
OFFLINE
DEPROVISIONED
REINITIALIZE GATEWAY

Card

type Restart Current

Software Load

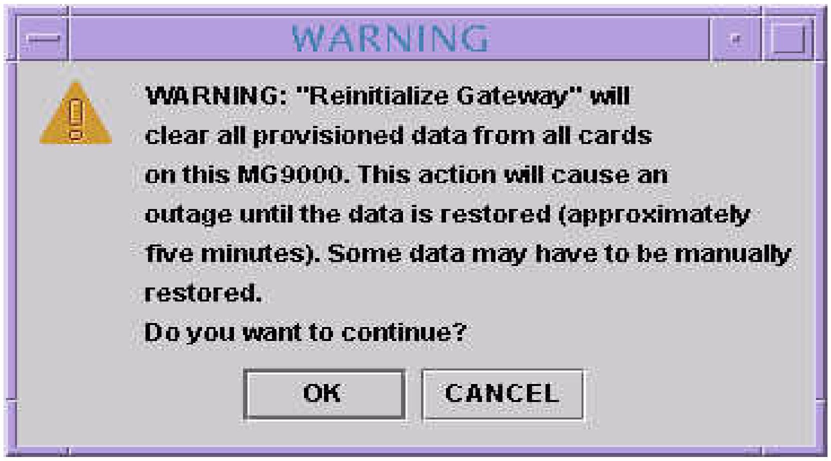
Restart Current:	OC3A04BC_GZ
Restart Flash Primary:	OC3A04BC_GZ
Restart Flash Backup:	unknown

OC3 Card Alarms | NE Info

Critical:	0	Minor:	0
Major:	0	Warning:	0

8 The system responds with the following warning message.

Warning message in response to Reinitialize Gateway command



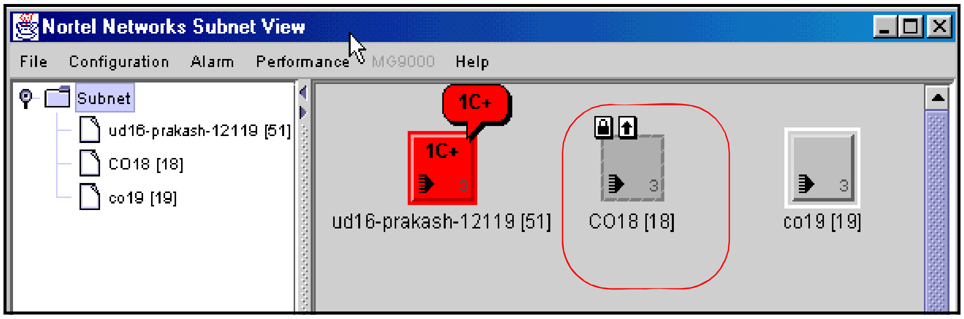
WARNING: "Reinitialize Gateway" will clear all provisioned data from all cards on this MG9000. This action will cause an outage until the data is restored (approximately five minutes). Some data may have to be manually restored.

Do you want to continue?

9 To continue, click OK and proceed to step 10. Otherwise click Cancel and go to step 11.

10 The MG 9000 responds with a Card State Change trap indicating that the configuration state is set to reinitialize and that the MG 9000 will clear persistence and restart. At the Subnet View, a “bomb” is displayed on the network element icon. After a period of time, the Subnet View is updated to show the up arrow indicating discovery and audit. When the operation is complete, the NE icon will be free of these added indicators. The following figure shows the NE is in discovery.

Subnet View showing degraded network element



The following NE606 log is output indicating that the Reinitialize Gateway action has been taken.

```
NE606 Wed Mar 20 12:38:52 EST 2002 INFO Reinitialize Gateway
Description: Reinitialize Gateway Event Sent
```

11 This procedure is complete.

Reinitializing intelligent cards in the MG 9000

When to use this procedure

Use this procedure when it is necessary to clear corrupted data out of intelligent cards in the MG 9000. This command is provided for situations where corrupted data is present on a pair of intelligent cards. This command is not for normal fault clearing activities. This command clears persistence data from the intelligent card and rebuilds that data from the MG 9000 Manager. If this command is used on the DCC cards, the entire network element is taken out of service and the data in persistence for the network element will be rebuilt from memory.

> ***Note:*** Perform the “Performing an MG 9000 data audit” procedure in *MG 9000 Configuration Management*, NN10096-511 before performing this procedure. Use of the Reinitialize command is highly disruptive and should only be used as a last resort.

The following intelligent cards have this capability:

- DCC (when the Reinitialize command is run on the DCC cards, the entire MG 9000 is reinitialized, as noted by the naming of the command Reinitialize Gateway as seen at the OC-3/DS1-IMA/GigE Card View)

  > ***Note:*** When it is necessary to reinitialize the DCC cards, use the Reinitialize the MG 9000 functionality procedure.

- ABI (DS-512)
- ITP
- DS1

> ***Note:*** The ITX card is not included in this capability because of a possibility of unrecoverable mismatch conditions. If the ITX cards need to be re-initialized, use the Reinitialize Gateway command from the DCC card.

Prerequisites

Because of the disruptive nature of the Reinitialize command, observe the following restrictions on the use of the Reinitialize command on intelligent cards in the MG 9000. The Reintialize command:

- is only allowed on active cards
- behaves like the Reinitialize Gateway command used in the DCC card

- runs a post reinitialize audit on the ITP and ABI card because of the switched lines data being handled on these cards
- does not run a post reinitialize audit on ITX cards
- runs a post reinitialize audit on DS1 cards because of the private lines data being handled by the DS1 card

Action

Reinitializing intelligent cards

At the MG 9000 Manager client

1

DANGER
Do not initiate any actions on affected GUIs until discovery of the card is complete.
When using the Reinitialize command on an intelligent card, if any GUIs are open, do not initiate any maintenance actions using those open GUIs other than to close them. This also applies to open VMG and termination GUIs when the ITP cards are reinitialized. Only initiate maintenance actions after discovery is complete.

From the SN08 Subnet View, double click on a network element (NE) that has been successfully upgraded to SN08 and for which the VMGs are to be upgraded. The Frame View appears.

2 From the Frame View, double click on the master shelf. The Shelf View appears.

3 Double-click on the active intelligent card to be reintialized. The Card View appears.

4 In the State pane, set the Administrative State to Locked.

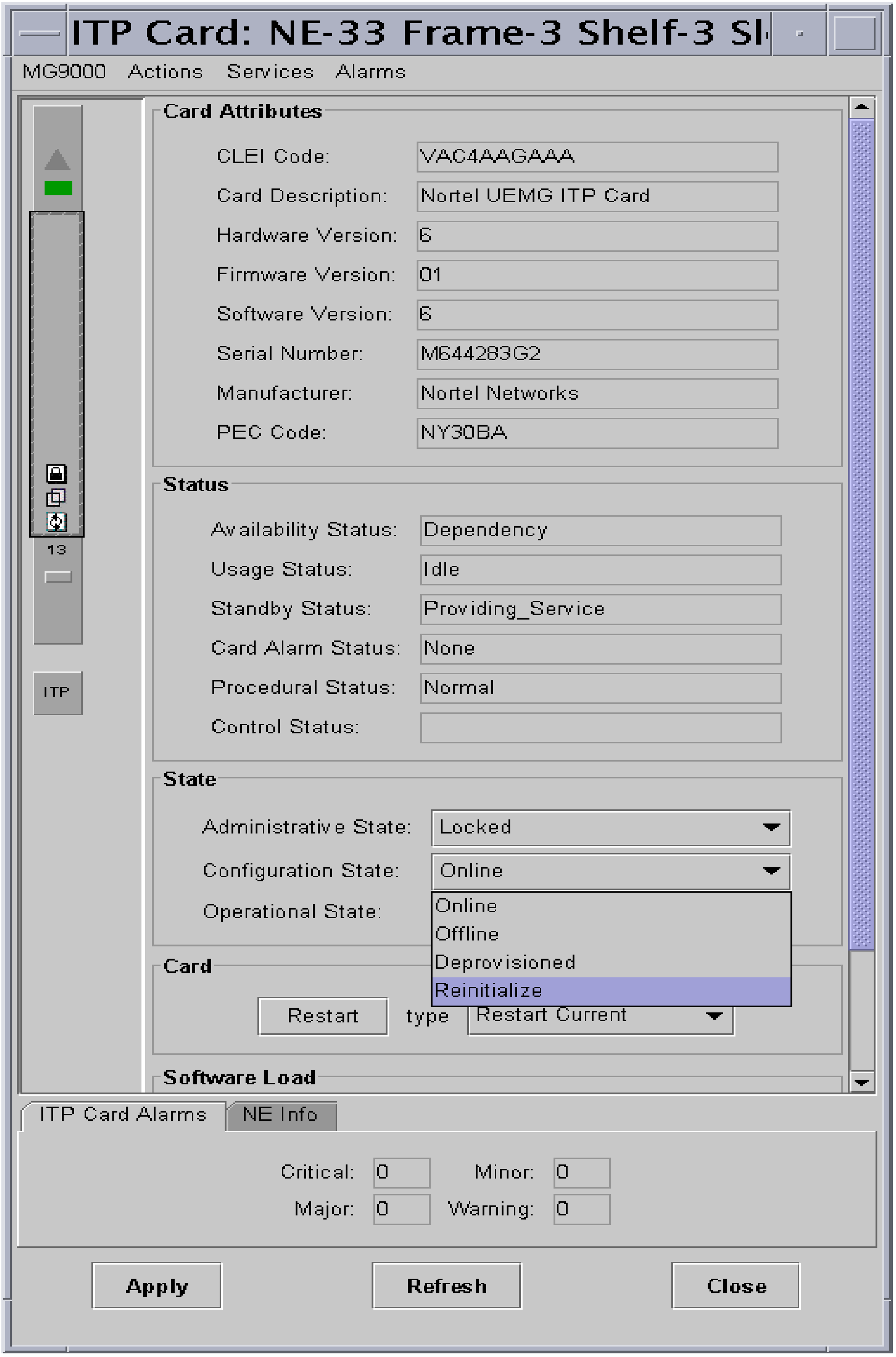
5

DANGER
The Reinitialize command is very disruptive to service.
Use the Reinitialize command as a last resort when all other attempts have failed, including running the Audit NE command available from the Configuration menu of the Subnet View. The Reinitialize command may interrupt call processing depending on the intelligent card chosen for reinitializing.

In the State pane, set the Configuration State to Reinitialize.

The following figure shows the location of the Reinitialize command.

Card View Reinitialize command



ITP Card: NE-33 Frame-3 Shelf-3 Sl

Card Attributes

CLEI Code: VAC4AAGAAA

Card Description: Nortel UEMG ITP Card

Hardware Version: 6

Firmware Version: 01

Software Version: 6

Serial Number: M644283G2

Manufacturer: Nortel Networks

PEC Code: NY30BA

Status

Availability Status: Dependency

Usage Status: Idle

Standby Status: Providing_Service

Card Alarm Status: None

Procedural Status: Normal

Control Status:

State

Administrative State: Locked

Configuration State: Online

Operational State:

Card

type Restart Current

Software Load

Critical: 0 Minor: 0

Major: 0 Warning: 0

6 Alarms will be raised at the Alarm Browser along with attending log reports that identify the state change of the cards being reintitialized reporting impacts on the MG 9000. The number and types of alarms depends on the cards selected to be reinitialized.

Wait for the cards to be recreated and the audit to complete.

7 In the State pane, set the Administrative State to Unlocked. This step will have to be repeated for all cards impacted by the reinitialize activity.

8 This procedure is complete.

Using the Clear persist and discover function

When to use this procedure

Use the following procedure to launch the Clear persist and discover (CPD) function from the MG 9000 Manager for a NE that has failed discovery.

This procedure is intended to allow you to establish communication with an undiscovered NE. The CPD function clears the configurable persistent data on the MG 9000 and reestablishes (rediscovers) the communication between the MG 9000 Manager and the NE.

When you use the CPD function, the system reports a NE606 log. For a description of the NE606 log, see *Carrier Voice over IP Logs Reference Manual*, NN10275-909.

Prerequisites

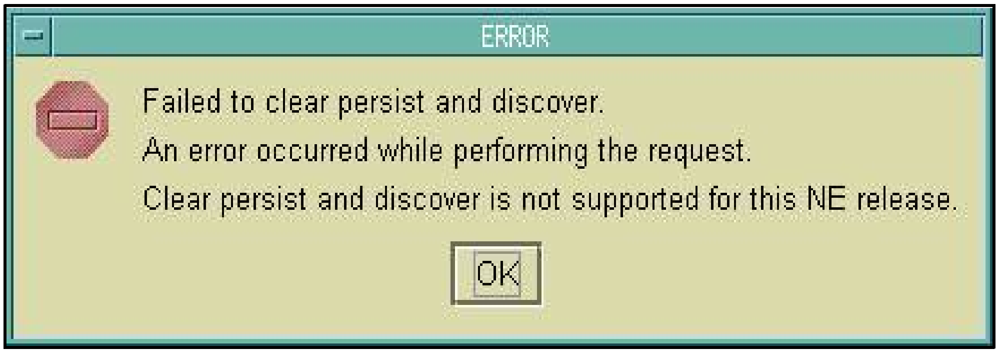
You must have administrative (emsadm) privileges to perform this procedure.

Limitations and restrictions

The following limitations and restrictions apply to this procedure:

- The SNMP communication channel must be operating for the CPD function to work.
- This procedure is valid for both discovered and undiscovered MG 9000 NEs, provided that the NE is running software configuration SN09FF and higher. If the NE is running a previous software release, the following error message is displayed:

Error Dialog



Failed to clear persist and discover.

An error occurred while performing the request.

Clear persist and discover is not supported for this NE release.

Action

CAUTION
Risk of service disruption and outage
The Clear persist and discover operation will disrupt service and result in an outage.

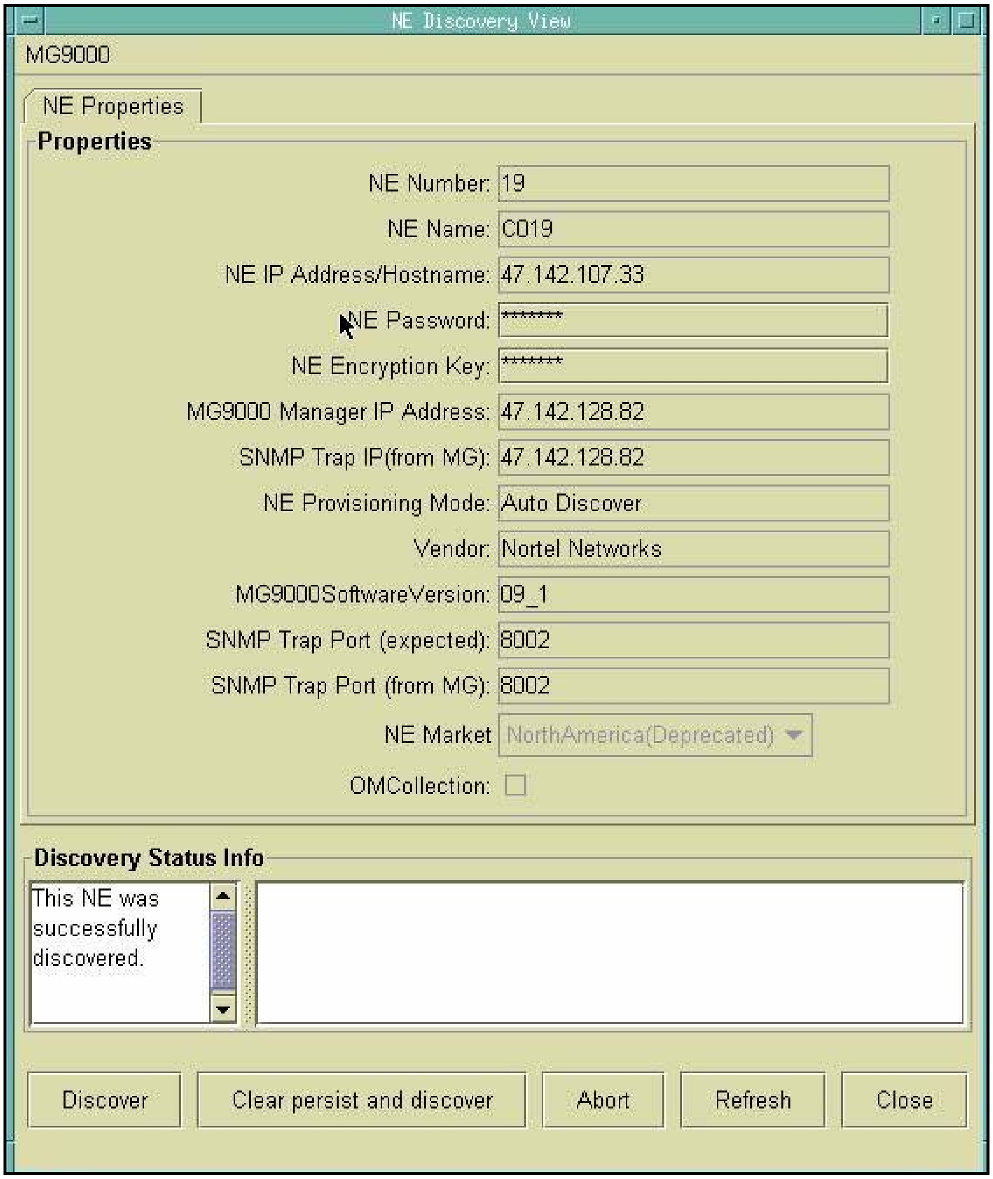
Using the Clear persist and discovery function

At the MG 9000 Manager

1 From the MG 9000 Manager Subnet view, select **Configuration > Discover NE**.

The NE Discovery view appears:

NE Discovery view



MG9000

NE Properties

Properties

NE Number: 19

NE Name: C019

NE IP Address/Hostname: 47.142.107.33

NE Password: *******

NE Encryption Key: *******

MG9000 Manager IP Address: 47.142.128.82

SNMP Trap IP(from MG): 47.142.128.82

NE Provisioning Mode: Auto Discover

Vendor: Nortel Networks

MG9000SoftwareVersion: 09_1

SNMP Trap Port (expected): 8002

SNMP Trap Port (from MG): 8002

NE Market NorthAmerica(Deprecated)

OMCollection: □

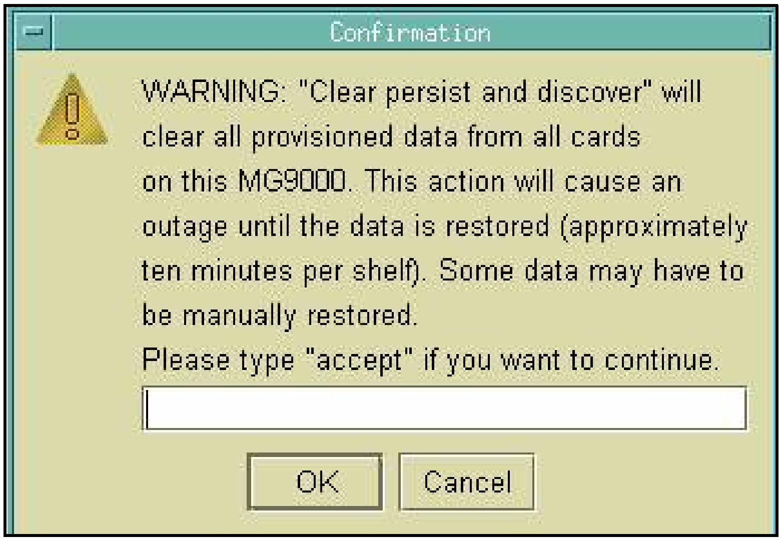
Discovery Status Info

This NE was successfully discovered.

2 Click the **Clear persist and discover** button at the bottom of the window.

The system asks you to confirm the operation:

Confirmation dialog



WARNING: "Clear persist and discover" will clear all provisioned data from all cards on this MG9000. This action will cause an outage until the data is restored (approximately ten minutes per shelf). Some data may have to be manually restored.

Please type "accept" if you want to continue.

3 If you accept this operation, service will be disrupted and an outage will occur on the NE.

If	Do
you want to continue	type "**accept**".
you do not want to continue	click **Cancel** to terminate the procedure.

4 Click **OK**.

The MG 9000 clears all of its persisted data and initiates a re-discovery of all hardware. When this discovery is complete, the MG 9000 sends a cold start trap to the MG 9000 Manager. The MG 9000 Manager will retrieve all hardware-related information and then start audit and recovery. As a part of audit and recovery, the MG 9000 Manager tries to restore all configuration data at the MG 9000.

5 You have completed this procedure.

Provisioning a connection using the LCI

When to use this procedure

The Connections menu at the LCI contains information necessary to add a newly configured MG 9000 to the network. Some common Connections menu tasks include the following actions:

- reconfiguring an AESA address in an MG 9000 network element to establish connection after SAM21 maintenance activity
- setting up connection to ATM network (Voice over AAL1 only)
- setting up call control connection
- setting up the OAMP connection between the MG 9000 and the MG 9000 Manager
- setting up ABI connection
- setting up DCC unit addresses (for GigE only)

Note: When changing LCI data on an active connection, there will be a loss of service. A message will appear warning of this condition.

Prerequisites

There are no prerequisites.

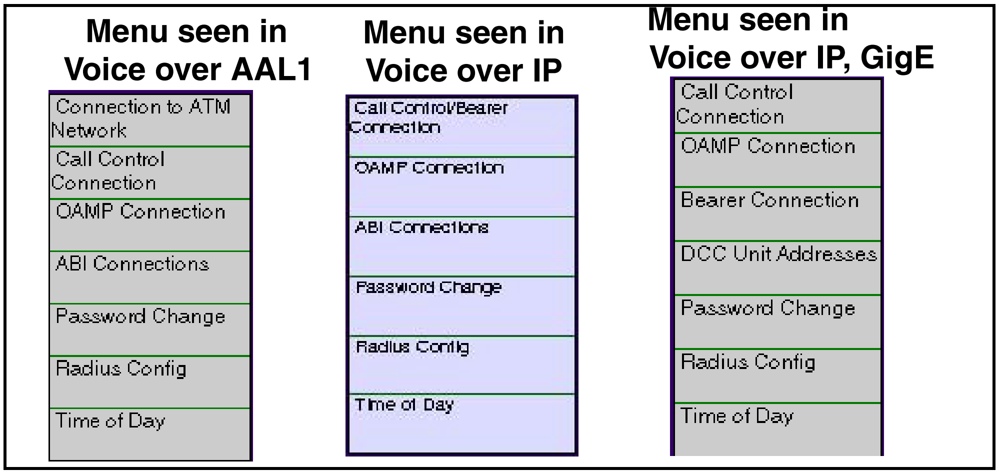
Action

Provisioning a connection using the LCI

From the LCI

1 Select the Connections button at the top right of the window to view a list of menu options.

Menu options seen by solution

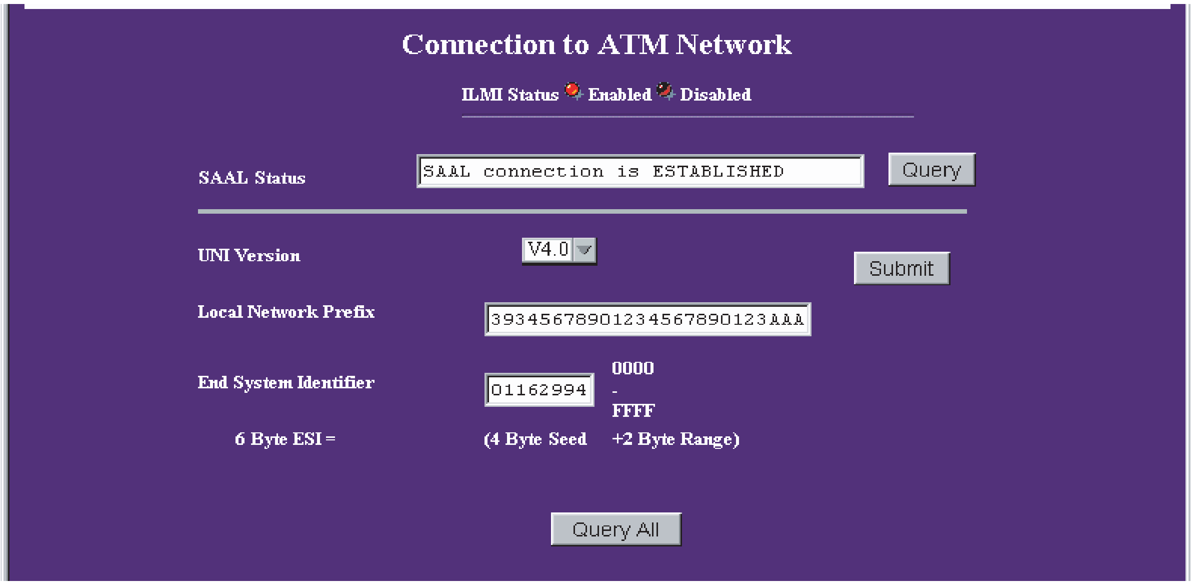


2 Use the information in the following table to determine the next step.

If the MG 9000 connection being provisioned is in a	Do
Voice over AAL1 solution	step 3
Voice over IP solution	step 5

3 Select Connection To ATM Network.

LCI screen showing connection to ATM network



Connection to ATM Network

ILMI Status ● Enabled ● Disabled

SAAL Status: SAAL connection is ESTABLISHED

UNI Version: V4.0

Local Network Prefix: 393456789012345678901230AAA

End System Identifier: 01162994 0000 - FFFF

6 Byte ESI = (4 Byte Seed +2 Byte Range)

4 Confirm that the ILMI status is Enabled and that the Local Network Prefix appears.

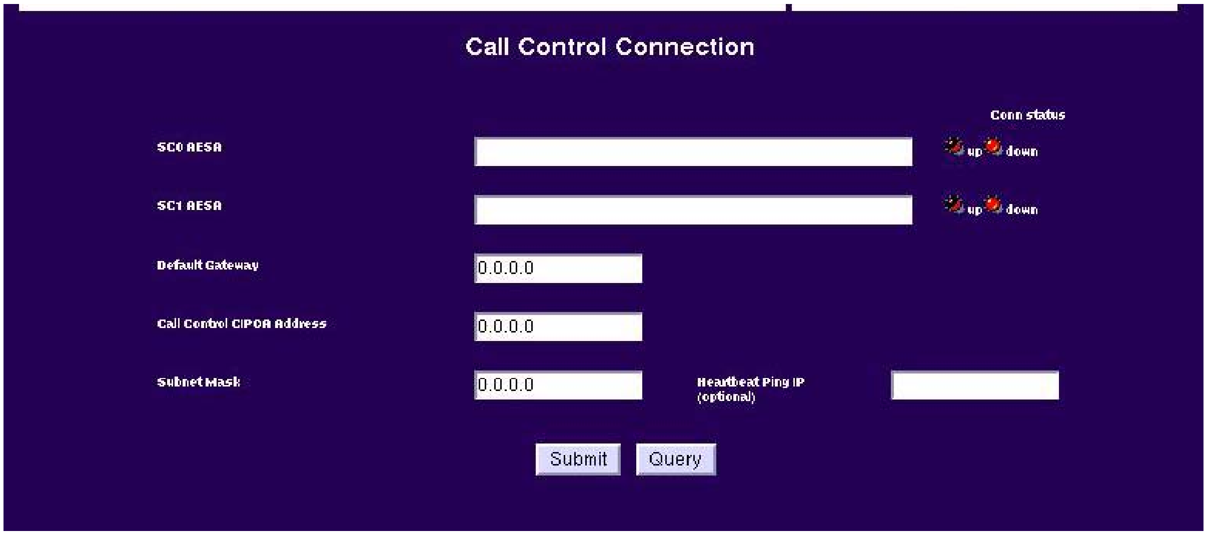
> ***Note:*** If the Local Network Prefix does not appear, do the following:
>
> - Select the UNI version 4.0.
> - Completely clear the Local Network Prefix field.
> - Select the submit button across from the UNI box.
> - A pop-up box delivers the Network Prefix.
> - The SAAL status indicates the connection is established.

5 Use the information in the following table to determine the next step.

If the MG 9000 connection being provisioned is in a	**Do**
Voice over AAL1 solution	step 6
Voice over IP solution	step 8
Voice over IP solution with GigE	step 9

6 Click on the Connections button and select Call Control Connection from the Menu options. The Call Control Connection LCI screen appears.

LCI screen showing Call Control Connection for Voice over AAL1



Call Control Connection

SC0 AESA:

SC1 AESA:

Default Gateway: 0.0.0.0

Call Control CIPOA Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Heartbeat Ping IP (optional):

a Enter or change the Primary AESA to SC0 and/or Secondary AESA to SC1 address.

b Enter the ‘Call Control CIPOA Address’.

c Enter the optional Heartbeat Ping IP address.

For information on the address to be entered in this field, refer to the "LCI Connections view" section and the description of the Heartbeat Ping IP address in *MG 9000 Configuration Management*, NN10096-511.

d Enter the Subnet Mask number: for example, 255.255.255.0.

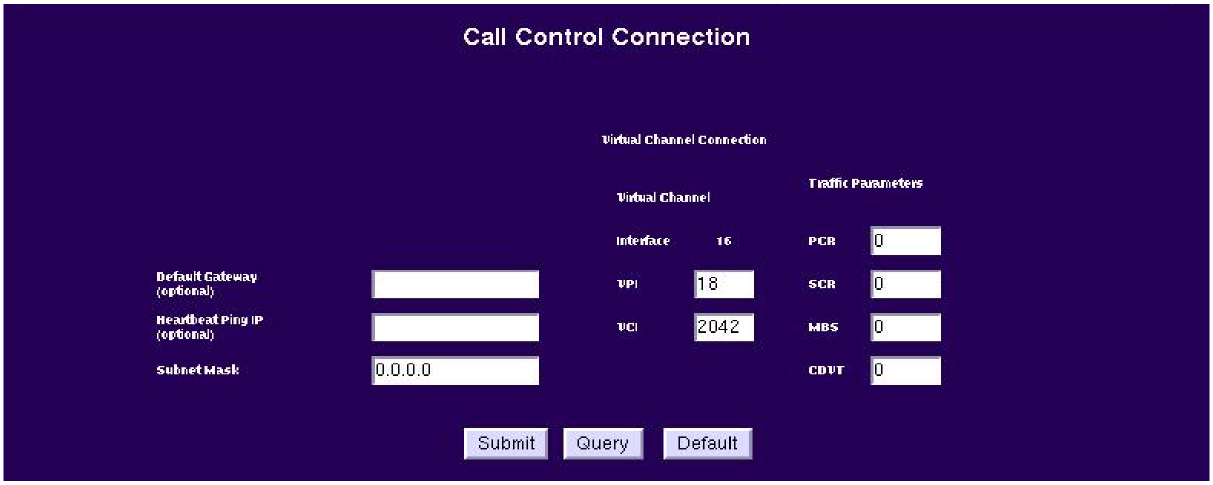
> ***Note:*** The Subnet Mask number is a value available from the operating company's IP specification book.

e Click on the Submit button to accept the changes.

7 Click on Query. If the data successfully allows a connection through the network to the Call Control server, the Up LEDs for each AESA will be lit. Go to step 10.

8 Click on the Connections button and select Call Control/Bearer Connection from the Menu options. The Call Control Connection screen appears.

LCI screen showing Call Control Connection for Voice over IP



Default Gateway (optional):

Heartbeat Ping IP (optional):

Subnet Mask: 0.0.0.0

Interface 16

VPI 18

VCI 2042

PCR 0

SCR 0

MBS 0

CDVT 0

a Enter the Default Gateway address

b Enter the Subnet Mask number: for example, 255.255.255.0.

> ***Note:*** The Subnet Mask number is a value available from the operating company's IP specification book.

c Enter the optional Heartbeat Ping IP address.

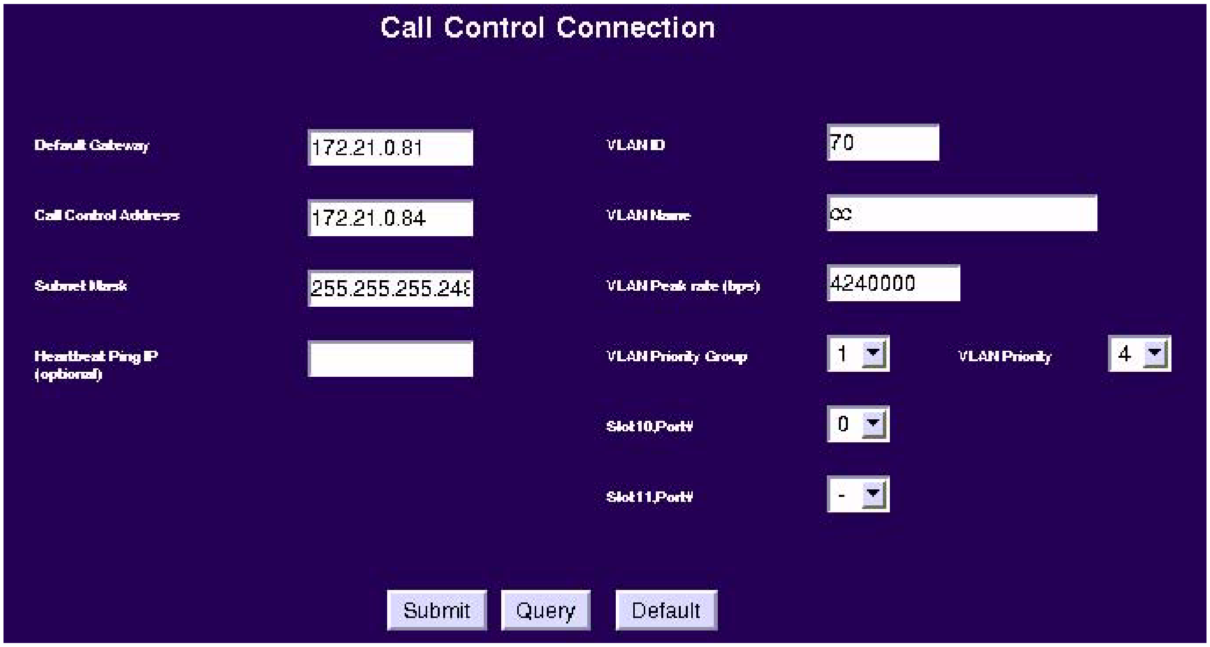
For information on the address to be entered in this field, refer to the "LCI Connections view" section and the description of the Heartbeat Ping IP address in *MG 9000 Configuration Management*, NN10096-511.

d Click on the Submit button to accept the changes.

e Click on Query. If the data successfully allows a connection through the network to the Call Control server, the Up LEDs for each AESA will be lit. Go to step 10.

9 Click on the Connections button and select Call Control Connection from the menu options. The Call Control Connections LCI screen appears.

LCI screen showing Call Control Connection for Voice over IP with GigE



Call Control Connection

Default Gateway	172.21.0.81	VLAN ID	70		
Call Control Address	172.21.0.84	VLAN Name	CC		
Subnet Mask	255.255.255.248	VLAN Peak rate (bps)	4240000		
Heartbeat Ping IP (optional)		VLAN Priority Group	1	VLAN Priority	4
		Slot10,Port#	0		
		Slot11,Port#	-		

a Enter the Default Gateway address

b Enter the Subnet Mask number: for example, 255.255.255.0.

> ***Note:*** The Subnet Mask number is a value available from the operating company’s IP specification book.

c Enter the optional Heartbeat Ping IP address.

For information on the address to be entered in this field, refer to the “LCI Connections view” section and the description of the Heartbeat Ping IP address in *MG 9000 Configuration Management*, NN10096-511.

d Enter the Call Control Address.

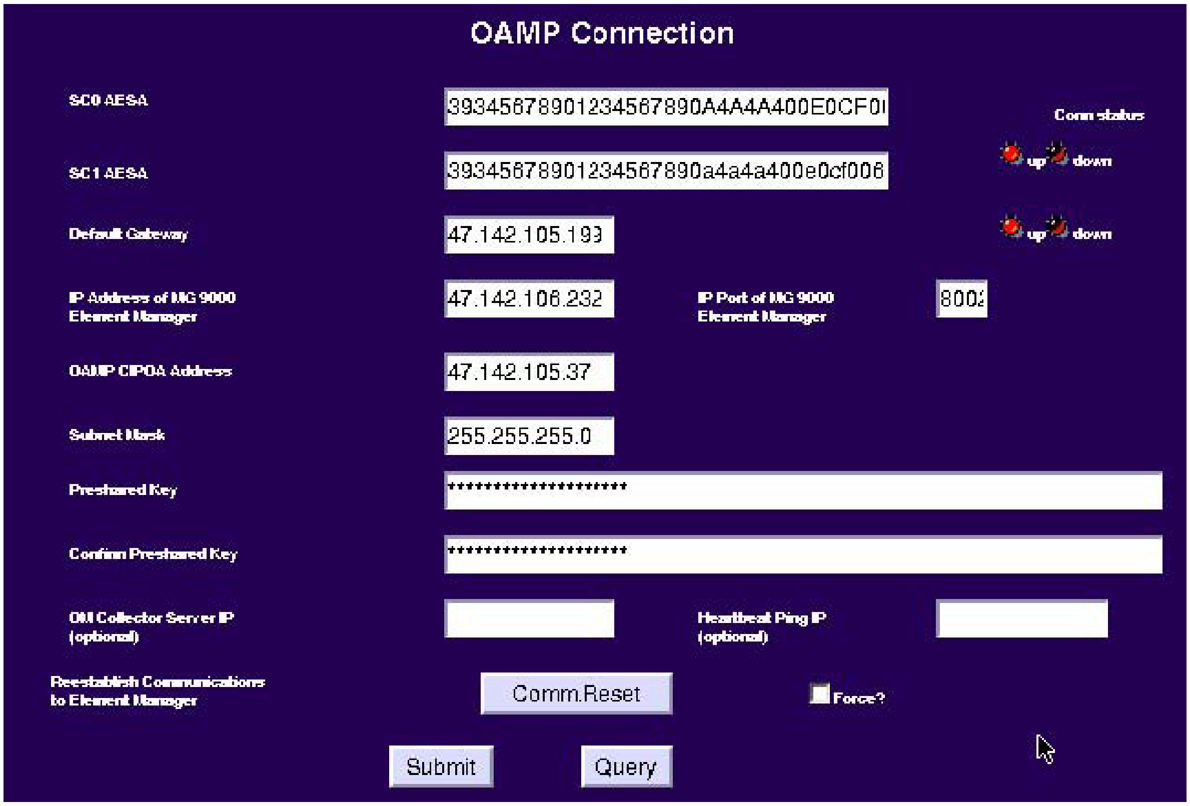
e Enter the virtual LAN (VLAN) ID, Peak Rate, Priority Group, and Priority. As an alternative, click on the Default button to select the default VLAN values.

f Enter the GigE DCC port number in slots 10 and 11

g Click on the Submit button to accept the changes.

10 Select the Connections button to view a list of menu options. Select OAMP Connection.

LCI screen showing OAMP connection for Voice over AAL1



OAMP Connection

SC0 AESA: 393456789012345678 90A4A4A400E0CF0(

SC1 AESA: 393456789012345678 90a4a4a400e0cf006

Default Gateway: 47.142.105.193

IP Address of MG 9000 Element Manager: 47.142.106.232

IP Port of MG 9000 Element Manager: 800(

OAMP CIPOA Address: 47.142.105.37

Subnet Mask: 255.255.255.0

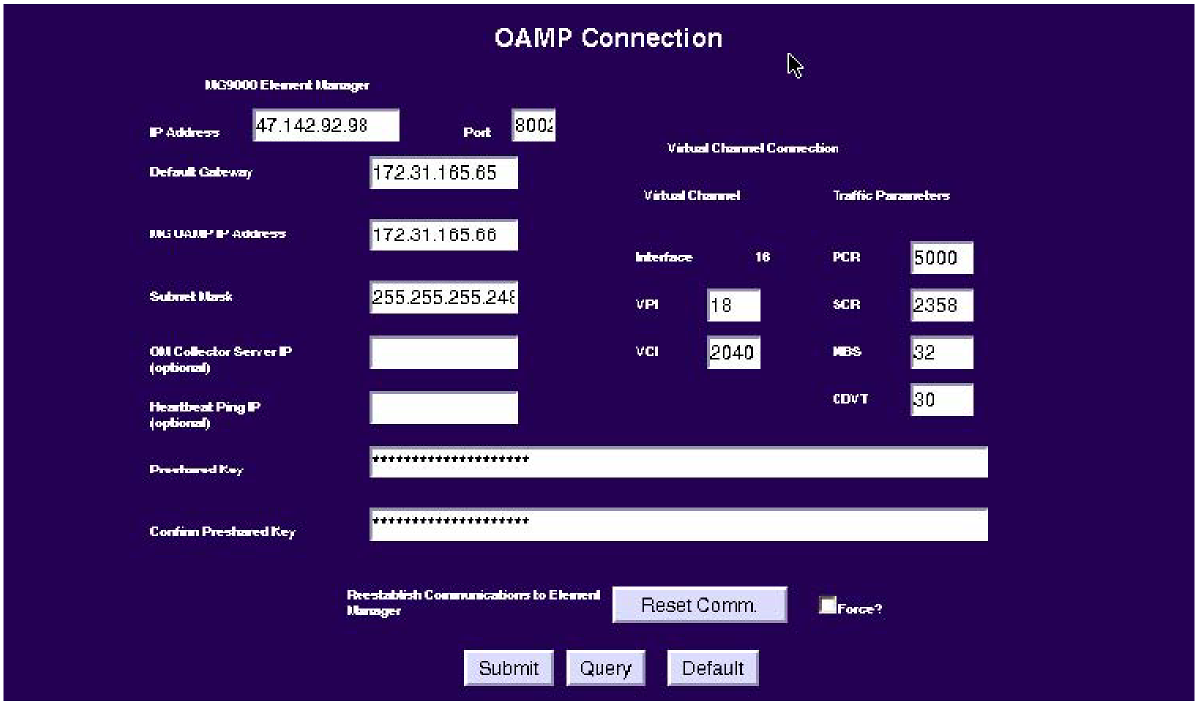
Preshared Key: ********************

Confirm Preshared Key: ********************

OM Collector Server IP (optional):

Heartbeat Ping IP (optional):

LCI screen showing OAMP connection for Voice over IP



OAMP Connection

MG9000 Element Manager

IP Address: 47.142.92.98

Port: 8002

Default Gateway: 172.31.165.65

MG OAMP IP Address: 172.31.165.66

Subnet Mask: 255.255.255.248

OM Collector Server IP (optional):

Heartbeat Ping IP (optional):

Preshared Key: ********************

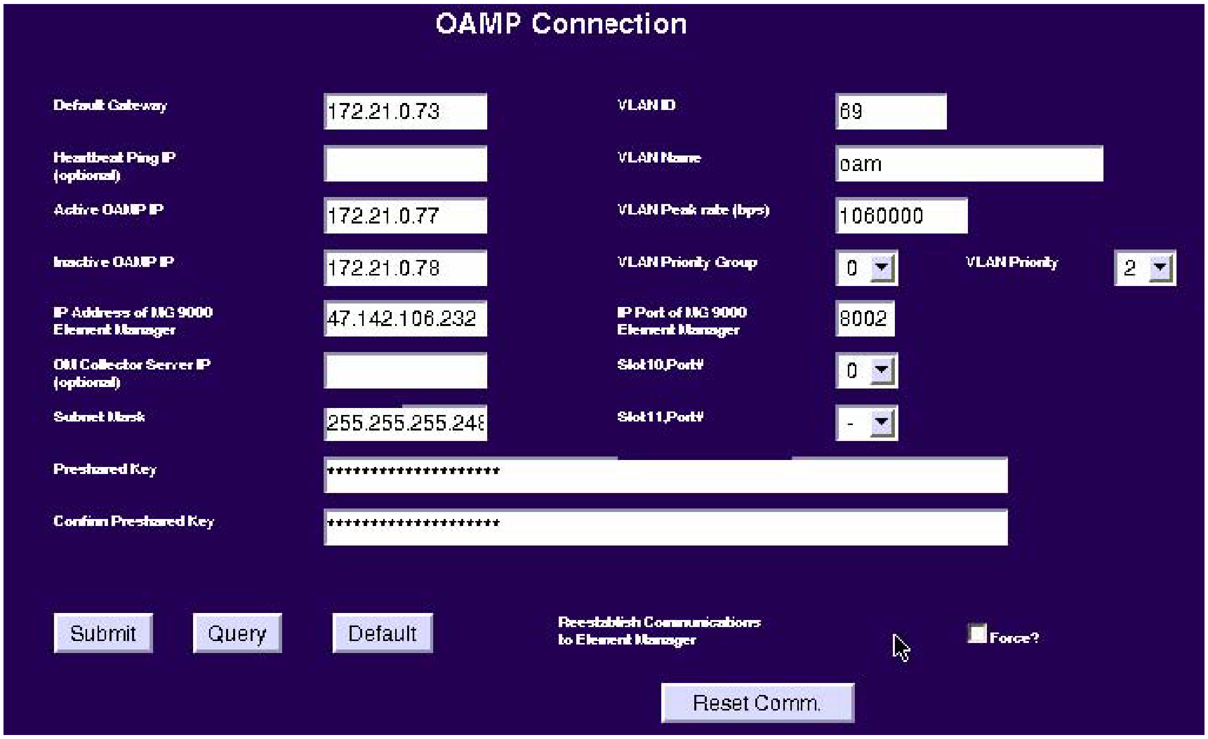
Confirm Preshared Key: ********************

Virtual Channel Connection

Virtual Channel		Traffic Parameters	
Interface	16	PCR	5000
VPI	18	SCR	2358
VCI	2040	MBS	32
		CDVT	30

Reestablish Communications to Element Manager

LCI screen showing OAMP connection for Voice over IP with GigE



OAMP Connection

Default Gateway: 172.21.0.73

Heartbeat Ping IP (optional):

Active OAMP IP: 172.21.0.77

Inactive OAMP IP: 172.21.0.78

IP Address of MG 9000 Element Manager: 47.142.106.232

OM Collector Server IP (optional):

Subnet Mask: 255.255.255.248

Preshared Key: ********************

Confirm Preshared Key: ********************

VLAN ID: 69

VLAN Name: oam

VLAN Peak rate (bps): 1060000

VLAN Priority Group: 0

VLAN Priority: 2

IP Port of MG 9000 Element Manager: 8002

Slot10,Port#: 0

Slot11,Port#: -

Reestablish Communications to Element Manager

Note: If operating the LCI from a workstation window and viewing a Subnet View Window, wait for the blue light in the Subnet View Window to stop flashing before continuing.

a For Voice over AAL1 only, enter or make necessary changes to the Primary AESA to SC0 and/or Secondary AESA to SC1.

b Enter the Default Gateway.

c Enter the IP address and port number of the MG 9000 Manager.

d Enter the OAMP CIPOA Address (for Voice over AAL1) or MG OAMP IP Address for (for Voice over IP).

e Enter the Subnet Mask, for example, 255.255.255.0.

Note: The Subnet Mask number is a value available from the operating company's IP specification book.

f For Voice over IP, no entries are required in the Virtual Channel Connection fields.

g Enter the OM Collector Server IP address.

h Enter the optional Heartbeat Ping IP address.

For information on the address to be entered in this field, refer to the "LCI Connections view" section and the description of the Heartbeat Ping IP address in *MG 9000 Configuration Management*, NN10096-511.

i For Voice over IP with GigE, enter the VLAN ID, VLAN name, VLAN Peak Rate, and VLAN Priority.

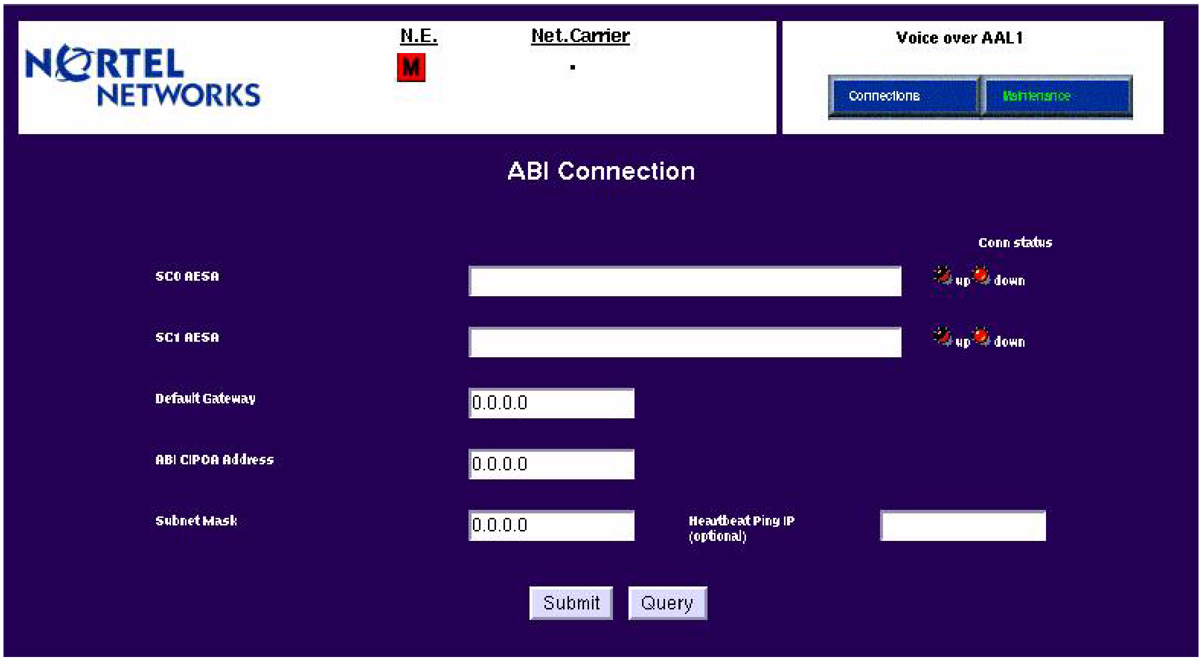
j For Voice over IP with GigE, enter the GigE DCC card port number for slots 10 and 11.

k Click on Submit button to accept the changes.

l Click on Query. For Voice over AAL1, if the data successfully allows a connection through the network on the Call Control Server, the Up LEDs for each AESA will be lit.

11 Select the Connections button to view of list of menu options and select ABI Connection, if the MG 9000 is provisioned with ABI (DS-512) cards and connection data must be changed. The ABI Connection screen appears.

LCI screen showing ABI Connection for Voice over AAL1



ABI Connection

SC0 AESA:

SC1 AESA:

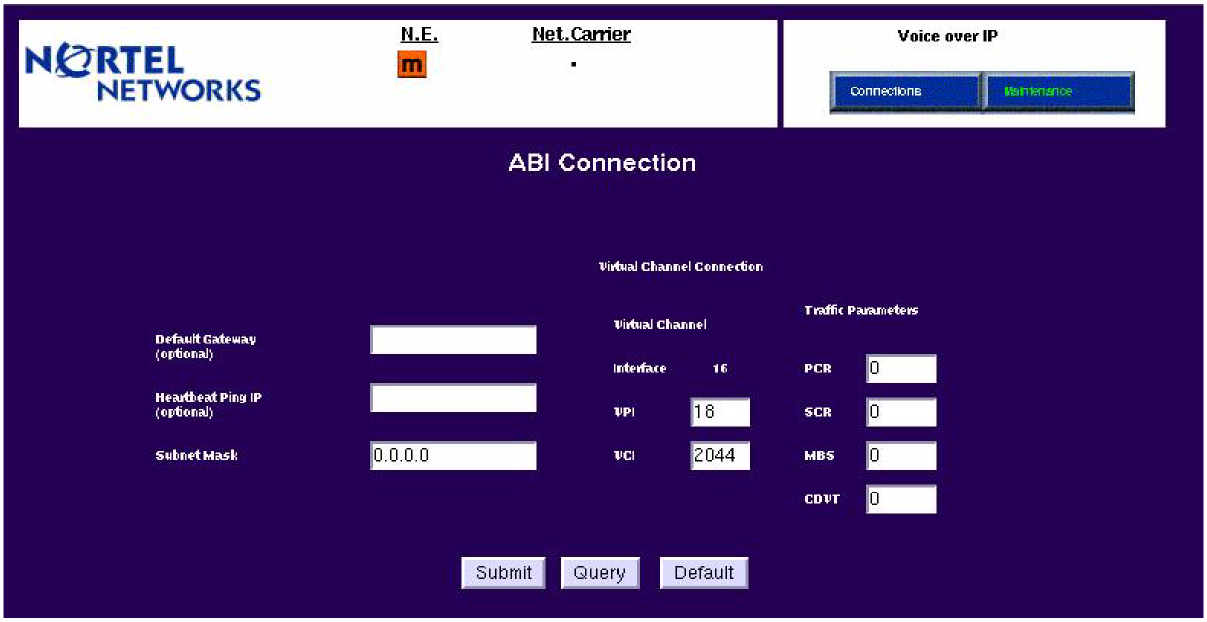
Default Gateway: 0.0.0.0

ABI CIPOA Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Heartbeat Ping IP (optional):

LCI screen showing ABI Connection for Voice over IP



ABI Connection

Default Gateway (optional):

Heartbeat Ping IP (optional):

Subnet Mask: 0.0.0.0

Virtual Channel Connection

Virtual Channel

Interface 16

VPI 18

VCI 2044

Traffic Parameters

PCR 0

SCR 0

MBS 0

CDVT 0

a For Voice over AAL1 only, enter or make necessary changes to the Primary AESA to SC0 and/or Secondary AESA to SC1.

b Enter the Default Gateway.

c For Voice over AAL1, enter the ABI CIPOA Address.

d Enter the optional Heartbeat Ping IP address.

For information on the address to be entered in this field, refer to the “LCI Connections view” section and the description of the Heartbeat Ping IP address in *MG 9000 Configuration Management*, NN10096-511.

e Enter the Subnet Mask.

f Click on Submit to accept the changes.

12 Click on Query. For Voice over AAL1, if the data successfully allows a connection through the network to the Gateway Controller, the Up LEDs for each AESA will be lit.

13 Select the Connections button to view a list of menu options and select Time of Day.

14 If necessary enter or change the current year, month, day, hour, minute and second. Select the Submit button.

15 This procedure is complete.

Manually imaging software for MG 9000 cards

Purpose of this procedure

Software imaging provides a means to upgrade an MG 9000 card, patch the card up to date, image the MG 9000 card load with the patches applied, and upgrade the rest of the cards of the same type in the office with the same load. This procedure provides the steps for the user to image one MG 9000 card at a time. To image multiple MG 9000 network elements, use the Network Patch Manager (NPM) interface.

> ***Note:*** Software imaging is performed through the NPM using the SmartImage Task command. For more information on the SmartImage Task command, refer to *UA-AAL1 Solution-level Basics*, NN10443-100-100 or *UA-IP Solution-level Basics*, NN10446-100.

The following MG 9000 cards (devices) are supported for software imaging:

- OC3 or DS1-IMA DCC card
- ITP card
- ITX card
- DS1 card
- ABI card

As part of the manual software image process, the MG 9000 Manager obtains patching information from the NPM. This information helps the user to determine if there is any reason the load in the card should not be imaged. If the NPM determines any of the following conditions, a warning message appears:

- the device (card) load contains obsolete patches
- the device (card) load contains patches that are on hold
- the device (card) is on hold
- the device (card) load is at a lower patch level than the previously imaged load

A failure message appears if communication with the NPM cannot be established.

> ***Note:*** The user has the ability to override these conditions and continue with the image process.

When to use this procedure

Typically the MG 9000 is imaged using the NPM imaging tools. Use this procedure when it is necessary to manually image the software on an MG 9000 card, as directed by Nortel Networks support.

Prerequisites

The user must have emsadm or emsrw permission.

Ensure the card to be imaged is patch current.

Ensure the floating IP address has already been provisioned.

Action

Manually imaging software for MG 9000 cards

At the MG 9000 Manager

1. From the Subnet View, select the network element (NE) containing the card to be imaged. Double-click on the NE icon. The NE window appears with the Frame View.
2. In the Frame View, double click on the shelf containing the card. The Shelf View appears.
3. In the Shelf View, double click on the card to be imaged. The Card View appears.
4. In the Card View, click on the Actions->Software Image menu item. The MG 9000 Software Image View appears as shown in the following figure.

Software Image view

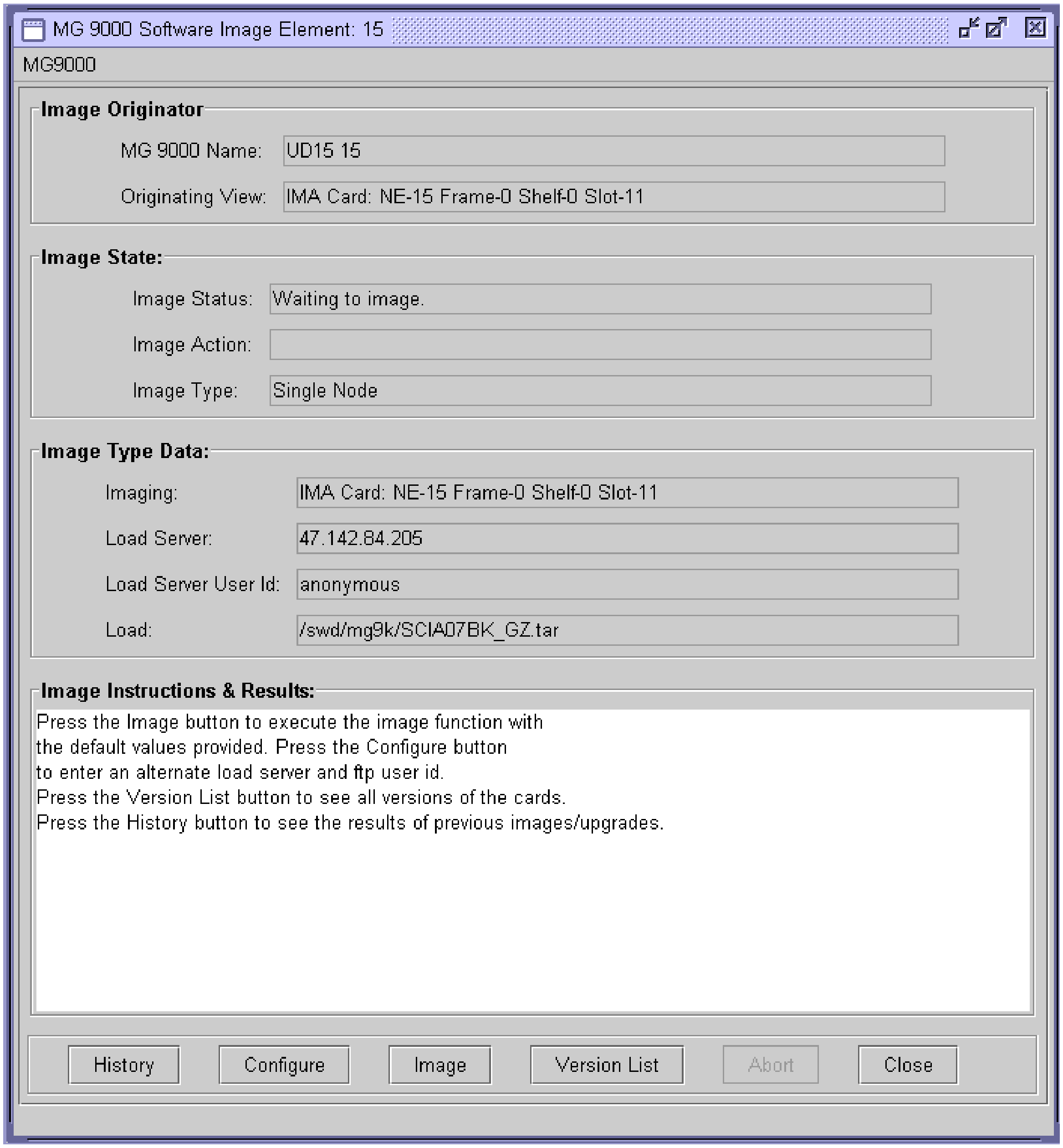


Image Originator

MG 9000 Name: UD15 15

Originating View: IMA Card: NE-15 Frame-0 Shelf-0 Slot-11

Image State:

Image Status: Waiting to image.

Image Action:

Image Type: Single Node

Image Type Data:

Imaging: IMA Card: NE-15 Frame-0 Shelf-0 Slot-11

Load Server: 47.142.84.205

Load Server User Id: anonymous

Load: /swd/mg9k/SCIA07BK_GZ.tar

Image Instructions & Results:

Press the Image button to execute the image function with
the default values provided. Press the Configure button
to enter an alternate load server and ftp user id.
Press the Version List button to see all versions of the cards.
Press the History button to see the results of previous images/upgrades.

5 Use the information in the following table to determine the next step.

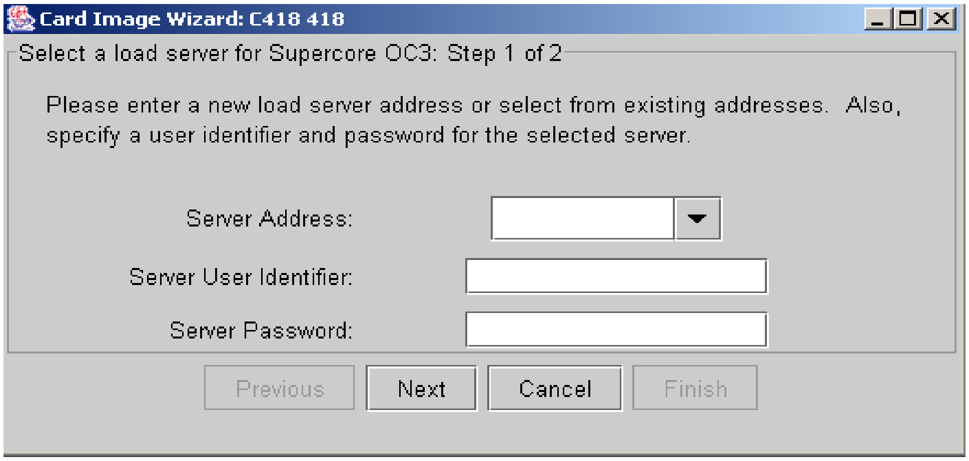
If the default server IP address, server userID, server password, or directory	Do
are to be used	step 6
are to be changed	step 7

6 Click on the Image button to begin the software image of the selected card using the default values provided in the Image Type Data pane.

Go to step 9

7 Click on the Configure button. The Card Image Wizard Select a load server: Step 1 of 2 appears as shown in the following figure.

Card Image Wizard, Select a load server: Step 1 of 2



Card Image Wizard: C418 418

Select a load server for Supercore OC3: Step 1 of 2

Please enter a new load server address or select from existing addresses. Also, specify a user identifier and password for the selected server.

Server Address:

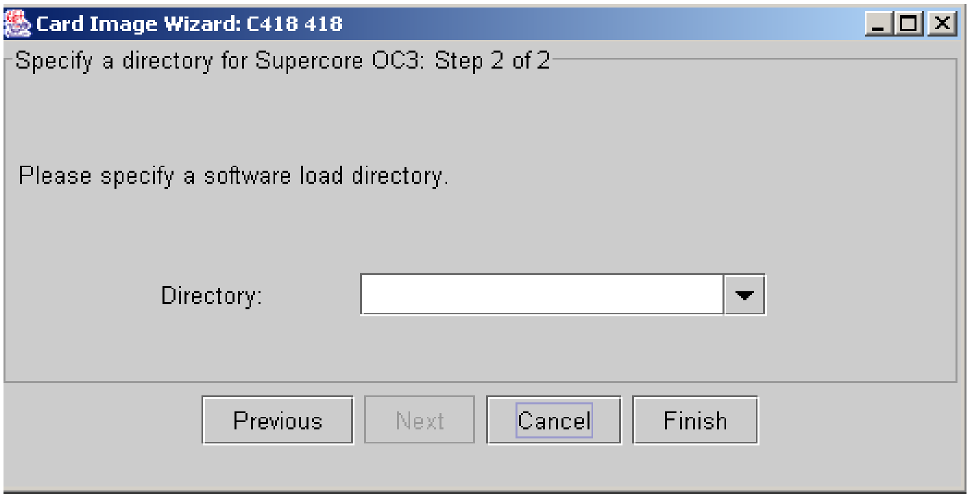
Server User Identifier:

Server Password:

From this wizard, the default server IP address, the server user identifier, and the server password can be changed. After all changes are made click Next. The Card Image Wizard Specify a directory: Step 2 of 2 appears as shown in the following figure.

> ***Note:*** Configure only changes values for the current session. It does not change default values permanently.

Card Image Wizard, Specify a directory: Step 2 of 2



Specify a directory for Supercore OC3: Step 2 of 2

Please specify a software load directory.

Directory:

From this wizard step, the default directory can be changed. Click Finish.

8 From the Software Image View click Image.

9 The Image Instructions & Results pane reports the results or any problems encountered. Follow the instructions in the pane to clear problems.

10 This procedure is complete.

Clearing MG 9000 alarms

This section identifies the various alarms that can be encountered at the MG 9000 Manager. Individual alarms output for cards in the MG 9000 shelf are categorized by card type. Each alarm is provided with the recovery methods. Each alarm message includes the following:

- alarm severity
- log report output in response to the alarm condition
- cause of the alarm
- actions required to clear the alarm

Fault type information

The fault type is part of the fault text sent to the MG 9000 Manager for NE300 alarms. The fault type will appear as a lead-in to the alarm description seen at the alarm browser. For example, when a hard fault is raised for the AAL5 SAR, the MG 9000 Manager will show: "hard fault for AAL5-SAR, Messaging".

The following are the defined alarm fault types and their descriptions and impacts:

- group - Group faults are raised when several related problems are reported. Group faults should not be seen by themselves. There will be other faults raised against the card that caused the group fault to be raised. The individual (hard, operational) faults may not be severe enough to cause a SWACT, but if many of these common minor faults are detected, a fault is raised against a group. The group faults are Major or Critical faults that will cause a SWACT when necessary.
- inferred - Inferred faults are raised when a minor software or hardware problem is detected several times during normal real-time operation.
- oper - Operational faults are raised when an application attempted a real-time action and failed. These faults can be hardware or software problems.
- hard - Hard faults are raised when diagnostics detect a problem. These faults are primarily hardware problems.
- restored - Restored faults are raised to report problems seen before a common (intelligent) card is restarted. A restored fault is a fault that was re-asserted against a card after a restart. Any node

maintenance fault will be restored if the fault is severe enough to cause a SWACT.

Using the previous example, if the card were to be restarted with the "hard fault for AAL5-SAR, Messaging" alarm raised, it would restore the fault. After the restart, the fault text will read: "restored fault for AAL5-SAR, Messaging".

Restored faults serve two purposes:

- They are a means of informing the customer through the MG 9000 Manager why the active card dropped activity. Previously, the active side would drop activity and restart. All faults would be cleared, providing no means of viewing fault history with the MG 9000 Manager.
- Restored faults will not be cleared until action is taken to fix the problem. This prevents problems that are seen only on the active side from causing SWACT loops.

Clearing restored faults:

- Diagnostics will not clear restored faults.The card with the restored faults may not be in the same state it was in before the restart that caused the faults to be restored.
- Restored faults require specific user action, regardless of the specific fault that is restored.
  - Fix the problem that caused the alarm. For example, replace a cable that is causing the fault.
  - Lock and Unlock the card, to cause a restart. When the card comes out of restart after being unlocked, no faults will be restored.

Clearing MG 9000 shelf alarms

Purpose of this procedure

This procedure identifies the alarms generated for the MG 9000 shelf, the alarm severity, the log report, the cause of the alarm, and the recovery methods. Shelf alarms are derived from faults detected by the DCC card, the SIC card and the alarm card in the BIP.

When to use this procedure

Use this procedure when an MG 9000 shelf alarm is raised in the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a shelf fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: shelfTalkBatteryA Severity: Critical Log: SHLF301	Cause: Shelf power problem, SIC talk battery A Action: Check the associated shelf’s talk battery connections, feeds, or fuses and replace any blown fuse and/or tighten any loose connection.
Type: shelfTalkBatteryB Severity: Critical Log: SHLF302	Cause: Shelf power problem, SIC talk battery B Action: Check the associated shelf’s talk battery connections, feeds, or fuses and replace any blown fuse and/or tighten any loose connection.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipTalkBatteryA1 Severity: Major Log: SHLF327	Cause: Frame power problem, talk battery A1 feed failure Action: Check for fuse failure at the frame or the power distribution cabinet (PDC) Check status of the associated Talk Battery filter card in the frame IBIP. Replace faulty fuse or, if power is available, replace Talk Battery A card. Go to Replace a dual talk battery filter card in an IBIP.
Type: bipTalkBatteryA2 Severity: Major Log: SHLF328	Cause: Frame power problem, talk battery A2 feed failure Action: Check for fuse failure at the frame or the power distribution cabinet (PDC) Check status of the associated Talk Battery filter card in the frame IBIP. Replace faulty fuse or, if power is available, replace Talk Battery A card. Go to Replace a dual talk battery filter card in an IBIP.
Type: bipTalkBatteryB1 Severity: Major Log: SHLF329	Cause: Frame power problem, B1 Talk Battery power feed failure Action: Check for fuse failure at the frame or the power distribution cabinet (PDC) Check status of the associated Talk Battery filter card in the frame IBIP. Replace faulty fuse or, if power is available, replace Talk Battery B card. Go to Replace a dual talk battery filter card in an IBIP.
Type: bipTalkBatteryB2 Severity: Major Log: SHLF330	Cause: Frame power problem, B2 Talk Battery power feed failure Action: Check for fuse failure at the frame or the power distribution cabinet (PDC) Check status of the associated Talk Battery filter card in the frame IBIP. Replace faulty fuse or, if power is available, replace Talk Battery B card. Go to Replace a dual talk battery filter card in an IBIP.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipAbsPowerSupply Severity: Critical Log: SHLF339	Cause: Alarm battery supply power problem Action: Check the associated frame's ABS battery connections/feeds or any power distribution frame fuses and replace any blown fuse and/or tighten any loose connection.
Type: shelfSignalBatteryA Severity: Major Log: SHLF303	Cause: Shelf power problem, fault in SIC signal battery A Action: Check the associated shelf's talk/signal battery connection feeds or fuses and replace any blown fuse or tighten any loose connection.
Type: shelfSignalBatteryB Severity: Major Log: SHLF304	Cause: Shelf power problem, fault in SIC signal battery B Action: Check the associated shelf's talk/signal battery connection feeds or fuses and replace any blown fuse or tighten any loose connection.
Type: shelfSignalBatteryAfuse Severity: Major Log: SHLF305	Cause: Shelf power problem, fault in SIC signal battery A Action: Check the associated shelf's talk/signal battery connection feeds or fuses and replace any blown fuse or tighten any loose connection.
Type: shelfSignalBatteryBfuse Severity: Major Log: SHLF306	Cause: Shelf power problem, fault in SIC signal battery B Action: Check the associated shelf's talk/signal battery connection feeds or fuses and replace any blown fuse or tighten any loose connection.
Type: shelfFailLED Severity: None Log: SHLF307	Cause: SIC card shelf fail LED Action: Check alarm browser for cause
Type: bipSignalBatteryA1 Severity: Major Log: SHLF308	Cause: Frame power problem, fault in BIP signal battery A1 Action: Check the associated frame's signal battery connections/feeds or fuses and replace any blown fuse and/or tighten any connection.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Shelf SIC card alarm Severity: Critical/Major/Minor Log: NE317	Type: Shelf SIC card alarm Action: Replace SIC card.
Type: Shelf PIO card alarm Severity: Critical/Major/Minor Log: NE317	Type: Shelf PIO card alarm Action: Replace power input/output (PIO) card.
Type: Shelf BIP card alarm Severity: Critical/Major/Minor Log: NE317	Type: Shelf BIP card alarm Action: Replace BIP card.
Type: bipSignalBatteryA2 Severity: Major Log: SHLF309	Cause: Frame power problem, fault in BIP signal battery A2 Action: Check the associated frame's signal battery connections/feeds or fuses and replace any blown fuse and/or tighten any connection.
Type: bipSignalBatteryB1 Severity: Major Log: SHLF310	Cause: Frame power problem, fault in BIP signal battery B1 Action: Check the associated frame's signal battery connections/feeds or fuses and replace any blown fuse and/or tighten any connection.
Type: bipSignalBatteryB2 Severity: Major Log: SHLF311	Cause: Frame power problem, fault in BIP signal battery B2 Action: Check the associated frame's signal battery connections/feeds or fuses and replace any blown fuse and/or tighten any connection.
Type: bipAbsFusefail Severity: Major Log: SHLF338	Cause: Frame power problem. Blown ABS fuse. Action: Replace blown ABS fuse on the face of the IBIP.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipCsApresence Severity: Major Log: SHLF341	Cause: Presence of BIP's Current-sense Card A. Action: Verify the presence of the associated Current Sense A card in the frame IBIP. Replace the Current Sense Card. Go to Replace a current sensor card in an IBIP If the alarm persists, replace the Alarm Processor Card. Go to Replace an alarm processor card in an IBIP.
Type: bipCsBpresence Severity: Major Log: SHLF342	Cause: Presence of BIP's Current-sense Card B. Action: Verify the presence of the associated Current Sense B card in the frame IBIP. Replace the Current Sense Card. Go to Replace a current sensor card in an IBIP If the alarm persists, replace the Alarm Processor Card. Go to Replace an alarm processor card in an IBIP.
Type: bipAlmRelayPresence Severity: Major Log: SHLF343	Cause: Presence of BIP's Alarm Relay Card. Action: Verify the presence of the Alarm Relay card in the frame IBIP. Replace the Alarm Relay Card. Go to Replace an alarm relay card in an IBIP If the alarm persists, replace the Alarm Processor Card. Go to Replace an alarm processor card in an IBIP.
Type: bipTalkBatteryA Severity: Minor Log: SHLF312	Cause: Frame power problem, fault in Talk Battery Filter A card Action: Replace Talk Battery Filter A card. Go to Replace a dual talk battery filter card in an IBIP.
Type: bipTalkBatteryB Severity: Minor Log: SHLF313	Cause: Frame power problem, fault in Talk Battery Filter B card Action: Replace Talk Battery Filter B card. Go to Replace a dual talk battery filter card in an IBIP.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipFilterA Severity: Minor Log: SHLF314	Cause: Frame power problem, BIP filter A failure Action: Replace Talk Battery Filter B card. Go to Replace a dual talk battery filter card in an IBIP.
Type: bipFilterB Severity: Minor Log: SHLF315	Cause: Frame power problem, BIP filter B failure Action: Replace Talk Battery Filter B card. Go to Replace a dual talk battery filter card in an IBIP.
Type: EcuTemp0 Severity: Minor Log: SHLF332	Cause: Lower half of frame temperature unacceptable Action: Check for tripped fan breaker, or alarm lights on fan drawer cover indicating fan failure. Check fan cable. Replace cooling unit if fan failure is evident. Go to Replacing a cooling unit.
Type: EcuTemp1 Severity: Minor Log: SHLF333	Cause: Upper half of frame temperature unacceptable Action: Check for tripped fan breaker, or alarm lights on fan drawer cover indicating fan failure. Check fan cable. Replace cooling unit if fan failure is evident. Go to Replacing a cooling unit.
Type: EcuFan0 Severity: Minor Log: SHLF334	Cause: Frame heating, ventilation, or cooling system problem. Fan cable disconnected. Action: Check for tripped fan breaker, or alarm lights on fan drawer cover indicating fan failure. Check fan cable. Replace cooling unit if fan failure is evident. Go to Replacing a cooling unit.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: EcuFan1 Severity: Minor Log: SHLF335	Cause: Frame heating, ventilation, or cooling system problem. Fan cable disconnected. Action: Check for tripped fan breaker, or alarm lights on fan drawer cover indicating fan failure. Check fan cable. Replace cooling unit if fan failure is evident. Go to Replacing a cooling unit.
Type: bipRemoteAlarmcutoff Severity: None Log: SHLF336	Cause: User has activated the remote alarm cutoff to silence remote alarms. Action: None, for information only.
Type: bipLocalAlarmcutoff Severity: None Log: SHLF337	Cause: User has activated the remote alarm cutoff to silence remote alarms. Action: None, for information only.
Type: bipScanPoint1, bipScanPoint2, bipScanPoint3, bipScanPoint4, bipScanPoint5, bipScanPoint6, bipScanPoint7, bipScanPoint8, bipScanPoint9, bipScanPoint10, bipScanPoint11 Severity: None, by default, but can be assigned Log: SHLF316 to 326	Cause: External equipment activation indicator. Action: Customer assignable scan points that are connected to external equipment. Check externally wired equipment based on what is defined for the scan point.
Type: bipCSAshf0HighThres Severity: Minor Log: SHLF344	Cause: Current-Sense Card A Shelf 0 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipCSAshf1HighThres Severity: Minor Log: SHLF345	Cause: Current-Sense Card A Shelf 1 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSAshf2HighThres Severity: Minor Log: SHLF346	Cause: Current-Sense Card A Shelf 2 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSAshf3HighThres Severity: Minor Log: SHLF347	Cause: Current-Sense Card A Shelf 3 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSBsh0HighThres Severity: Minor Log: SHLF348	Cause: Current-Sense Card B Shelf 0 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipCSBsh1HighThres Severity: Minor Log: SHLF349	Cause: Current-Sense Card B Shelf 1 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSBsh2HighThres Severity: Minor Log: SHLF350	Cause: Current-Sense Card B Shelf 2 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSBsh3HighThres Severity: Minor Log: SHLF351	Cause: Current-Sense Card B Shelf 3 High Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high current threshold (approximately 11 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipTempHighThres Severity: Minor Log: SHLF352	Cause: Current High Temperature Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the high temperature threshold (158 ° F).
Type: bipCSAshf0LowThres Severity: Minor Log: SHLF353	Cause: Current-Sense Card A Shelf 0 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipCSAshf1LowThres Severity: Minor Log: SHLF354	Cause: Current-Sense Card A Shelf 1 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSAshf2LowThres Severity: Minor Log: SHLF355	Cause: Current-Sense Card A Shelf 2 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSAshf3LowThres Severity: Minor Log: SHLF356	Cause: Current-Sense Card A Shelf 3 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSBsh0LowThres Severity: Minor Log: SHLF357	Cause: Current-Sense Card B Shelf 0 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipCSBsh1LowThres Severity: Minor Log: SHLF358	Cause: Current-Sense Card B Shelf 1 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSBsh2LowThres Severity: Minor Log: SHLF359	Cause: Current-Sense Card B Shelf 2 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipCSBsh3LowThres Severity: Minor Log: SHLF360	Cause: Current-Sense Card B Shelf 3 Low Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low current threshold (approximately 9 A). The system still initiates current limiting actions, reducing the loop current on a per line basis as needed.
Type: bipTempLowThres Severity: Minor Log: SHLF361	Cause: Current LowTemperature Threshold exceeded Action: None, for information only. This alarm reports that the associated threshold has exceeded the low temperature threshold (32 ° F).
Type: bipSignalBatteryFuse Severity: Major Log: SHLF362	Cause: Status of the Signal Battery Fuse Action: Check the associated fuse at the frame IBIP. The fuses contain a light emitting diode (LED) which illuminates when the fuse is blown. Replace the faulty fuse to clear the trouble.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipTalkBatteryAFuse Severity: Major Log: SHLF363	Cause: Status of Talk Battery A fuse. Action: Check the associated fuse at the frame IBIP. The fuses contain a light emitting diode (LED) which illuminates when the fuse is blown. Replace the faulty fuse to clear the trouble.
Type: bipTalkBatteryBFuse Severity: Major Log: SHLF364	Cause: Status of Talk Battery B fuse. Action: Check the associated fuse at the frame IBIP. The fuses contain a light emitting diode (LED) which illuminates when the fuse is blown. Replace the faulty fuse to clear the trouble.
Type: bipECUFuse0 Severity: Minor Log: SHLF365	Cause: Status of cooling unit 0 fuse. Action: Check the associated fuse at the frame IBIP. The fuses contain a light emitting diode (LED) which illuminates when the fuse is blown. Replace the faulty fuse to clear the trouble.
Type: bipECUFuse1 Severity: Minor Log: SHLF366	Cause: Status of cooling unit 1 fuse. Action: Check the associated fuse at the frame IBIP. The fuses contain a light emitting diode (LED) which illuminates when the fuse is blown. Replace the faulty fuse to clear the trouble.
Type: bipEndAisleFuse Severity: Minor Log: SHLF367	Cause: Status of the End Aisle fuse. Action: Check the associated fuse at the frame IBIP. The fuses contain a light emitting diode (LED) which illuminates when the fuse is blown. Replace the faulty fuse to clear the trouble.
Type: bipSignalDistribution1 Severity: None, by default, but can be assigned Log: SHLF368	Cause: BIP Signal Distribution Point 1. Action: Customer assignable distribution point which can be used to drive external equipment.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipSignalDistribution2 Severity: None, by default, but can be assigned Log: SHLF369	Cause: BIP Signal Distribution Point 2. Action: Customer assignable distribution point which can be used to drive external equipment.
Type: bipSignalDistribution3 Severity: None, by default, but can be assigned Log: SHLF370	Cause: BIP Signal Distribution Point 3. Action: Customer assignable distribution point which can be used to drive external equipment.
Type: bipSignalDistribution4 Severity: None, by default, but can be assigned Log: SHLF371	Cause: BIP Signal Distribution Point 4. Action: Customer assignable distribution point which can be used to drive external equipment.
Type: bipVisualCritical Severity: None Log: SHLF372	Cause: Frame equipment malfunction audible. indicator. Action: None, for information only.
Type: bipVisualMajor Severity: None Log: SHLF373	Cause: Frame equipment malfunction audible. indicator. Action: None, for information only.
Type: bipVisualMinor Severity: None Log: SHLF374	Cause: Frame equipment malfunction audible. indicator. Action: None, for information only.
Type: bipAudibleCritical Severity: None Log: SHLF375	Cause: Frame equipment malfunction audible. indicator. BIP Audible Critical alarm sounds. Action: None, for information only.
Type: bipAudibleMajor Severity: None Log: SHLF376	Cause: Frame equipment malfunction audible. indicator. BIP Audible Major alarm sounds. Action: None, for information only.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipAudibleMinor Severity: None Log: SHLF377	Cause: Frame equipment malfunction audible. indicator. BIP Audible Minor alarm sounds. Action: None, for information only.
Type: bipAlarmCutOffLED Severity: N/A Log: SHLF378	Cause: BIP Alarm CutOff LED Action: None, for information only.
Type: bipTBFailALED Severity: N/A Log: SHLF379	Cause: BIP Talk Battery Fail A LED Action: None, for information only.
Type: bipTBFailBLED Severity: N/A Log: SHLF380	Cause: BIP Talk Battery Fail B LED Action: None, for information only.
Type: bipCriticalLEDbank Severity: N/A Log: SHLF381	Cause: Frame visual indicator of a critical equipment malfunction. Action: None, for information only.
Type: bipMajorLEDbank Severity: N/A Log: SHLF382	Cause: Frame visual indicator of a major equipment malfunction. Action: None, for information only.
Type: bipMinorLEDbank Severity: N/A Log: SHLF383	Cause: Frame visual indicator of a minor equipment malfunction. Action: None, for information only.
Type: bipEcu1LED Severity: N/A Log: SHLF384	Cause: BIP environmental control unit 0 LED. Visual indication of a heating, ventilation, or cooling system problem. Action: None, for information only.
Type: bipEcu2LED Severity: N/A Log: SHLF385	Cause: BIP environmental control unit 1 LED. Visual indication of a heating, ventilation, or cooling system problem. Action: None, for information only.

Shelf alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: bipAlarmFailLED Severity: N/A Log: SHLF386	Cause: BIP alarm processor card fail LED. Frame alarm equipment malfunction. Action: Check all cabling to the IBIP.
Type: bipAisleAlarm Severity: N/A Log: SHLF387	Cause: Visual indicator used to located the aisle which has the equipment malfunction. Action: None, for information only.
Type: bipFrameFail Severity: N/A Log: SHLF388	Cause: BIP Frame Fail Action: None, for information only.
Type: bipAlarmRelayLed Severity: N/A Log: SHLF389	Cause: Presence of BIP’s Alarm Relay Card Action: None, for information only.
Type: bipCsAled Severity: N/A Log: SHLF390	Cause: Status of Current Sense Card A LED Action: None, for information only.
Type: bipCsBled Severity: N/A Log: SHLF391	Cause: Status of Current Sense Card B LED Action: None, for information only.
Type: shelfCompatibility Severity: Minor Log: SHLF392	Cause: A shelf compatibility fault is received from the MG 9000 Manager server. Action: Insert a compatible card in the slot adjacent to its mate.
Type: cardDiscovery Severity: Minor Log: SHLF393	Cause: A card discovery, card discovery power input/output (I/O), card discovery power shelf interface card (SIC), or card discovery slot (2-21) fault is received from the MG 9000 Manager server. Action: Insert a good card in the slot represented in the fault message.

Clearing MG 9000 DCC card alarms

Purpose of this procedure

This procedure identifies the alarms generated for the DCC card (OC-3, DS1-IMA, or GigE), the alarm severity, the log report, the cause of the alarm, and the recovery methods. DCC alarms are derived from faults detected by the DCC card.

When to use this procedure

Use this procedure when MG 9000 DCC card alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a DCC fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: AtmDataSyncRsrc Severity: Critical Log: NE302	Cause: ATM data sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BalDataSyncRsrc Severity: Critical Log: NE302	Cause: BAL data sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: MegacoDataSyncRsrc Severity: Critical Log: NE302	Cause: MEGACO data sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: NEDataSyncRsrc Severity: Critical Log: NE302	Cause: NE data sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BaseSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Base Platform Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: CarmSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Carrier Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: NodeSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Node Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MegacoSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Megaco Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: DLMSubsystmRsrc Severity: Critical Log: NE302	Cause: Startup failure: Data Line Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: TestSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Test Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MTASubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: MTA Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ShfSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Shelf Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: LineSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Line Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ClkSyncSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Clock Sync Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: PatchSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Patching Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: DTASubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: DTA Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: MegOmsSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Megaco OMs Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: SnmpMASubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: SNMP Master Agent Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: TimeSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Time of Day Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: TestRsrc Severity: Critical Log: NE302	Cause: Test Resource Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: SCLocalBusRamRsrc Severity: Major Log: NE301	Cause: Local Memory Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: FlashRsrc Severity: Major Log: NE301	Cause: Flash Memory Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ScLinePortUnstableRsrc Severity: Major Log: NE305	Cause: The rate of Signal State Change Interrupt (SSI) messages on the affected card exceeds a safe operational threshold. Action: If the alarm affects an active card, the alarm causes a SWACT, which changes the state of the card to inactive. Monitor the inactive card for 1hour. If the alarm occurs on an inactive card, and no further link faults occur, the system clears the alarm automatically after 1 hour. If the system does not clear the alarm on an inactive card after 1 hour, replace the card.
Type: SCLineLinkRsrc Severity: Minor Log: NE304	Cause: Link to master shelf ITP in slot (12, 13) - isolation in progress; link to Mate DCC - isolation in progress; link to card in slot (2-8, 14-21) isolation in progress Action: Two cards cannot communicate with each other. Diagnostics will isolate the fault and determine the course of action. The alarm will change to an NE305 within 3 minutes.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: EXT_LINK Severity: Minor Log: NE304	Cause: Hard fault for link to card in slot (2) isolation in progress Action: Perform the following steps: • Lock/unlock card A, the more subordinate card. For example, if the cards are ITP/ITX, then the ITP is card A; if the cards are DCC/Other, then the Other card is card A. • Lock/unlock card B • Replace card A • Put the old card A back and replace card B • Examine the link If the fault is on and ITP or ITX card, the link between the cards is a tangible entity that can be replaced. When replacing the cable, make sure that it is attached to the inactive ITX (it may be necessary to SWACT ITX cards), and install a new card. ***Note:*** Do not attempt to repair connectors on cables attached to powered-up cards. The soldering iron will short the pins and possibly damage the card. For other cards (such as ABI to DCC, DS1 to DCC, or ITX to DCC), if the link is between cards in the master shelf, all the links cross the backplane. Visually inspect the backplane and look for bent or damaged pins.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCLineExternalRsrc Severity: Minor Log: NE305	Cause: External: master shelf ITP in slot (12, 13); External mate DCC card; External: card in slot (2-9, 14-21) Action: Check the far end slot for card alarms. If alarms exist, clear those alarms. If no alarms exist on far end slot or there are only External alarms on the far end slot, there is a backplane problem between the far end card and the DCC card. Reseat the other card in question to see if the alarm clears. If that does not clear the alarm, reseat the DCC card.
Type: SCLineIntercardRsrc Severity: Minor Log: NE305	Cause: Backplane connection to master shelf ITP (12, 13); unused backplane connection; backplane connection to mate DCC card; backplane connection to card in slot (2-9, 14-11) Action: Check the far end slot for card alarms. If alarms exist, clear those alarms. If no alarms exist on far end slot or there are only External alarms on the far end slot, there is a backplane problem between the far end card and the DCC card. Reseat the other card in question to see if the alarm clears. If that does not clear the alarm, reseat the DCC card.
Type: SCQuadSerContGrpRsrc Severity: Major Log: NE305	Cause: Group of Serial Ports Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: SCNetworkIfRsrc Severity: Major Log: NE301	Cause: Network Interface ***Note:*** Applies only to the DCC-OC-3 card. Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCNetworkIfRsrc Severity: Major Log: NE301	Cause: Network Interface (0-7) ***Note:*** Applies only to the DCC DS1-IMA card. Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: SCOCardNEProxy or SCIcardNEProxy Severity: Major Log: NE318	Cause: SCI or SCO card NE proxy. Card communication failure. Proxy mode activated. Action: Perform the following steps: 1. Wait a about 2 minutes to see if the alarm clears on its own. The alarm may be caused by a restart or any break in communication that may clear automatically. 2. Check the alarm log report to see if the active C-side path has any faults. If so, follow the alarm clearing procedures for those faults. If an active DCC card has faults that affect downstream communication, all subtending cards will have the Proxy fault. Clear the DCC fault before attempting to clear Proxy faults on other cards. 3. Lock and offline the card. Unseat the card from the backplane, then reseat it. 4. Repeat step 1. If the alarm does not clear then replace the card. Go to Replacing a DCC card. After replacing the card, repeat step 1. If the alarm still does not clear, call Nortel Networks for support.
Type: SCAtmFwdRsrc Severity: Critical Log: NE301	Cause: ATM cell forwarder Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCWanBldrOAMPRsrc Severity: Major Log: NE308	Cause: Inband Messaging OAMP Link (0 or 1), inband messaging OAMP PVC Action: The MG 9000 Manager is down. Perform the following: • Check for alarms on shelf controller. • Use LCI to verify that AESA provisioning information is correct. • If the problem persists, call your next level of support.
Type: SCLinePortRsrc Severity: Minor Log: NE305	Cause: Serial Device (0, 1) to Master Shelf ITP in slot (12, 13); Serial Device 3 - Link to Mate DCC card; Serial Device (4-19) - to card is slot (2-9, 14-21) Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: SCAtmCPCSUniRsrc Severity: Major Log: NE302	Cause: CPCS UNI Signaling Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: MateCommunicationRsrc Severity: Critical Log: NE302	Cause: Mate card communication failure Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: FileDescRsrc Severity: Major Log: NE302	Cause: File Descriptors Low Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCWanBldrCCRsrc Severity: Major Log: NE308	Cause: Inband Messaging CC Link (0 or1), inband messaging CC PVC Action: The MG 9000 Manager is down. Perform the following: • Check for alarms on shelf controller. • Use LCI to verify that AESA provisioning information is correct. • If the problem persists, call your next level of support.
Type: SCWanBldrOAMPHBRsrc Severity: Major Log: NE308	Cause: Heartbeat on OAMP connection Action: The MG 9000 Manager is down. Perform the following: • Check for alarms on shelf controller. • Use LCI to verify that AESA provisioning information is correct. • If the problem persists, call your next level of support.
Type: SCWanBldrCCHBRsrc Severity: Major Log: NE308	Cause: Heartbeat on Call Control Connection Action: The MG 9000 Manager is down. Perform the following: • Check for alarms on shelf controller. • Use LCI to verify that AESA provisioning information is correct. • If the problem persists, call your next level of support.
Type: SCWanBldrDS512Rsrc Severity: Major Log: NE308	Cause: Inband Messaging DS512 Link (0 or 1), inband messaging DS512 PVC Action: The MG 9000 Manager is down. Perform the following: • Check for alarms on shelf controller. • Use LCI to verify that AESA provisioning information is correct. • If the problem persists, call your next level of support.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCWanBldrDS512HBRsrc Severity: Major Log: NE308	Cause: Heartbeat on DS512 connection Action: The MG 9000 Manager is down. Perform the following: • Check for alarms on shelf controller. • Use LCI to verify that AESA provisioning information is correct. • If the problem persists, call your next level of support.
Type: SCBitsFwdRsrc Severity: Major Log: NE309	Cause: BITS forwarder Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCBitsRefRsrc Severity: Major Log: NE309	Cause: BITS clock reference (A or B) Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: SCLinksRsrc Severity: Major Log: NE315	Cause: Resource Bandwidth Action: Some of the carriers are not providing bandwidth.Verify and fix any CARRIER alarms. If problem persists, restart the card.
Type: SCTimeOfDayRsrc Severity: Minor Log: NE311	Cause: Time of Day: Access to time server (IP) failed Action: Attempts to access the provisioned time server have failed. Perform the following: • Verify the provisioned IP address of the time server is correct. • Verify time server is operational and online. • Use the LCI to re-submit the Time of day parameters. This forces immediate time server access.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCXcRsrc Severity: Minor Log: NE314	Cause: Backplane Cross Connect Action: The carriers between the two DCC cards cannot communicate. Use the following information to clear the alarm. Verify and fix any Carrier alarms. If seen on Active DCC: • Restart the inactive DCC. • If problem persists, replace inactive DCC. Go to Replacing a DCC card. • If problem persists, call next level of support. If seen on inactive DCC: • Restart the inactive DCC. • If problem persists, SWACT the DCC cards. This will cause carriers to go down momentarily. Be sure to call next level to verify it is permissible to SWACT. • Restart the newly inactive DCC card. • If problem persists, replace the newly inactive card. Go to Replacing a DCC card. • If problem persists, call next level of support. If both DCCs have this fault, there is a backplane problem in the shelf. Replace the entire shelf backplane. Contact Nortel Networks.
Type: SCSWRsrc Severity: Minor Log: NE301	Cause: ATM Switch - MMC Chipset Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCQuadsercontPortRsrc Severity: Minor Log: NE310	Cause: Serial Port (0, 1) - Unused link to ITP card in slot (12, 13) Action: If fault is on both ITPs: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card.
Type: SCOctalPhyContPortRsrc Severity: Warning Log: NE311	Cause: Unused Octal PHY Port (0-15) ***Note:*** Applies only to the DCC-OC-3 card. Action: Unused hardware alarms can be safely ignored. ***Note:*** Attempt to clear the alarm before the next software upgrade, since the new software may use more hardware than the old software load. Respond to the alarm as follows: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: SCOctalPhyContRsrc Severity: Warning Log: NE311	Cause: Unused Octal PHY Device for ports (0-5) or (8-13) ***Note:*** Applies only to the DCC-OC-3 card. Action: Unused hardware alarms can be safely ignored. ***Note:*** Attempt to clear the alarm before the next software upgrade, since the new software may use more hardware than the old software load. Respond to the alarm as follows: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: SCBootFlashMemRsrc Severity: Warning Log: NE301	Cause: Flash Memory containing software load Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: SCEthernetIfRsrc Severity: Warning Log: NE301	Cause: Ethernet port Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: SCTerminalIfRsrc Severity: Warning Log: NE301	Cause: RS-232 port Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: CardTypeMismatchRsrc Severity: Critical Log: NE301	Cause: Idprom Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: IdpromRsrc Severity: Major Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: CardPairOOSRsrc Severity: Warning Log: NE301	Cause: Active/Master Card Out of Service Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: RedundancyLostRsrc Severity: Warning Log: NE301	Cause: Simplex Mode - No Redundancy Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DCC card.
Type: norNodeSwact Severity: None Log: NE500	Cause: Card has performed a switch of activity (SWACT). Action: None, for information only.
Type: norNodeStateChange Severity: None Log: NE501	Cause: Card has performed a state change. Action: None, for information only.
Type: ovldDetectionAlarm Severity: Minor/Major Log: OVLD304	Cause: This alarm is generated when an overload detection alarm is received from an MG 9000. Indicates a performance trouble has occurred. Action: Calls may be lost. Check the resource usage for this network element.
Type: ovldRscMonPduRateFault Severity: Warning Log: OVLD800	Cause: This alarm is generated when an Pdu rate overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ovldRscMonCbvMsgRFault Severity: Warning Log: OVLD801	Cause: This alarm is generated when an Cbv message rate overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: ovldRscMonConnQueFault Severity: Warning Log: OVLD802	Cause: This alarm is generated when an connection queue overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: ovldRscMonCpuUtilFault Severity: Warning Log: OVLD803	Cause: This alarm is generated when an CPU utilization fault is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: perfMonCpuFault Severity: Warning Log: OVLD804	Cause: This alarm is generated when a CPU utilization overloaded alarm is received from an MG 9000. Action: None, for information only.
Type: perfMonRamFault Severity: Warning Log: OVLD805	Cause: This alarm is generated when a PM RAM utilization fault is received from an MG 9000. Action: None, for information only.
Type: perfMonFlashFault Severity: Warning Log: OVLD806	Cause: This alarm is generated when a PM flash utilization fault is received from an MG 9000. Action: None, for information only.
Type: perfMonChannFault Severity: Warning Log: OVLD807	Cause: This alarm is generated when a PM channel utilization fault is received from an MG 9000. Action: None, for information only.
Type: TalkBatteryFeedALowVoltage Severity: Major Log: NE317	Cause: This alarm is generated when the low voltage threshold has been set or the alarm has cleared for Talk Battery Feed A. Action: None, for information only.

DCC card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: TalkBatteryFeedBLowVoltage Severity: Major Log: NE317	Cause: This alarm is generated when the low voltage threshold has been set or the alarm has cleared for Talk Battery Feed B. Action: None, for information only.
Type: TalkBatteryFeedAOops Severity: Major Log: NE317	Cause: This is the office oscillation phenomena signal (OOPS) alarm for talk battery feed A. When this alarm occurs, the current limit will be incrementally lowered from 50 mA to 40 mA to 30 mA and finally to 23 mA. If after lowering the current limit the alarm still exists, the cross talk fix is disabled. This will allow line circuits that do not have active calls to be powered down. This alarm is also output when the condition clears. Action: None, for information only.
Type: TalkBatteryFeedBOops Severity: Major Log: NE317	Cause: This is the office oscillation phenomena signal (OOPS) alarm for talk battery feed B. When this alarm occurs, the current limit will be incrementally lowered from 50 mA to 40 mA to 30 mA and finally to 23 mA. If after lowering the current limit the alarm still exists, the cross talk fix is disabled. This will allow line circuits that do not have active calls to be powered down. This alarm is also output when the condition clears. Action: None, for information only.
Type: PatchAlarmFault Severity: Major Log: PATC301	Cause: This alarm is generated when a patch alarm fault is received on an MG 9000 DCC card indicating a restart is required after a patch has been removed or applied. Action: Restart the affected card by performing the procedure Restarting a card on page 348.

The ports on the DCC card are mapped as shown in the following table.

DCC port mapping

Serial port number	Mapped to
Port 0	ITP in Slot 13 (currently unused)
Port 1	ITP in Slot 12 (currently unused)
Port 2	Unused
Port 3	Link to mate DCC card
Port 4	Link to card in slot 2
Port 5	Link to card in slot 6
Port 6	Link to card in slot 14
Port 7	Link to card in slot 18
Port 8	Link to card in slot 3
Port 9	Link to card in slot 7
Port 10	Link to card in slot 15
Port 11	Link to card in slot 19
Port 12	Link to card in slot 4
Port 13	Link to card in slot 8
Port 14	Link to card in slot 16
Port 15	Link to card in slot 20
Port 16	Link to card in slot 5
Port 17	Link to card in slot 9
Port 18	Link to card in slot 17
Port 19	Link to card in slot 21

Clearing MG 9000 GigE link alarms

Purpose of this procedure

This procedure identifies the alarms generated for the GigE DCC card links, the alarm severity, the log report, the cause of the alarm, and the recovery methods. GigE link alarms are derived from faults detected by the GigE DCC card.

When to use this procedure

Use this procedure when MG 9000 GigE DCC card link alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a GigE link fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

GigE link alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Loss of signal Severity: Critical Log: GIGE301	Cause: Network Problem - Loss of signal Action: Indicates a far-end problem. Check the far-end equipment.
Type: Remote failure indication Severity: Critical Log: GIGE302	Cause: Network Problem - Remote failure indication Action: Indicates a far-end equipment failure. Check the far-end equipment.
Type: Transmit failure indication Severity: Critical Log: GIGE303	Cause: Network Problem - Transmit failure Action: The transmitter in the NTTP62CF GigE LX small-form factor pluggable (SFP) transceiver has failed. Replace the SFP on the affected link. Refer to Replacing an NTTP62 SFP transceiver device on page 414.

GigE link alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Temperature Threshold Exceeded Severity: Critical Log: GIGE304	Cause: Network Problem - Temperature Threshold Exceeded Action: The NTTP62CF SFP operating temperature is beyond its limits. Replace the SFP on the affected link. Refer to Replacing an NTTP62 SFP transceiver device on page 414.
Type: Low Power Indicated Severity: Critical Log: GIGE305	Cause: Network Problem - Low Power Indicated Action: Power level in the NTTP62CF SFP is below required minimum. Replace the SFP on the affected link. Refer to Replacing an NTTP62 SFP transceiver device on page 414.
Type: Receive Signal Degraded Severity: Critical Log: GIGE306	Cause: Network Problem - Receive Signal Degraded Action: Errored frames were received from the far-end equipment. Check the far-end network. Possible fiber or NTTP62CF SFP problem on MG 9000, network, or far-end equipment.
Type: Receive Excessive Error Ratio Severity: Critical Log: GIGE307	Cause: Network Problem - Receive Excessive Error Ratio Action: Excessive errored-frames were received. Points to an equipment problem. Check fibers and SFPs on the MG 9000, far-end, and intermediate equipment (such as, fiber patch panel).
Type: Transmit Bias Current Severity: Critical Log: GIGE308	Cause: Network Problem - Transmit Bias Current Action: Transmit bias current is beyond limits. Replace the NTTP62CF SFP on the affected link. Refer to Replacing an NTTP62 SFP transceiver device on page 414.

GigE link alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Link Integrity Failure Severity: Critical Log: GIGE309	Cause: Network Problem - Link Integrity Failure Action: No communication with the mate GigE DCC card. Check the condition of the mate GigE DCC card. With this alarm, there is typically a problem in the network related to the card for which the alarm is raised. Check for other alarms and check the health of the network link for which it is raised.
Type: Transmit Optical Power Severity: Critical Log: GIGE310	Cause: Network Problem - Transmit Optical Power is too low. Action: Replace the NTTP62CF SFP on the affected link. Refer to Replacing an NTTP62 SFP transceiver device on page 414.
Type: Receive Optical Power Severity: Critical Log: GIGE311	Cause: Network Problem - Receive Optical Power Action: Not receiving sufficient receive signal over the fiber. Check the far-end equipment or fiber connections.
Type: Network Failure Severity: Critical Log: GIGE313	Cause: Network Problem - Network Failure (LKINT) Action: There is a problem in the network. Most likely, communication between the two edge routers is down, but do not rule out other network issues.
Type: Auto Negotiation Failure Severity: Major Log: GIGE314	Cause: Network Problem - Auto Negotiation Failure Action: Check the setup on far-end equipment; ensure Auto-Negotiation is enabled. Verify the far-end equipment is operating. If the fault cannot be cleared, replace the GigE DCC card.

GigE link alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Non Preferred Link is active Severity: Minor Log: GIGE315	Cause: Network Problem - Non Preferred Link is Active Action: Check setup, clear any network problems, SWACT to the mate GigE DCC card. The non-preferred link alarm is raised only if link reversion is provisioned. The alarm will be raised when the link provisioned as the protection link becomes the active link. When the problem on the preferred link clears, a soak timer is started. The cards automatically SWACT at the end of the soak time if the problem is not cleared. This will clear the alarm so there is no need for a manual SWACT.
Type: Link Invalid alarm Severity: Critical Log: GIGE316	Cause: Network Problem - Link Invalid alarm Action: There is an equipment problem. Check end to end connectivity (for example, fiber cables, connections, or SFPs at both ends).
Type: No Protection Group Redundancy Severity: Minor Log: GIGE317	Cause: Network Problem - No Protection Group Redundancy Action: Mainly a provisioning alarm that is raised when there is not a completely provisioned protection group (that is, two network interface links in the protection group, with both unlocked and in service). It is also raised if a link goes out of service.

Clearing MG 9000 ITX card alarms

Purpose of this procedure

This procedure identifies the alarms generated for the ITX card, the alarm severity, the log report, the cause of the alarm, and the recovery methods. ITX alarms are derived from faults detected by the ITX card.

When to use this procedure

Use this procedure when MG 9000 ITX card alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with an ITX fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser.
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appear in the Description field.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: AtmDataSyncRsrc Severity: Critical Log: NE302	Cause: ATM Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: UpgSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Software Upgrade Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: NodeSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Node Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: TestRsrc Severity: Critical Log: NE302	Cause: Test Resource Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BaseSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Base Platform Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MegacoDataSyncRsrc Severity: Critical Log: NE302	Cause: Megaco Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BalDataSyncRsrc Severity: Critical Log: NE302	Cause: BAL Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: TestSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Test Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: FileDescRsrc Severity: Major Log: NE302	Cause: File Descriptors Low Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: DataMismatchRsrc Severity: Critical Log: NE302	Cause: Data Mismatch with DCC Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: MateCommunicationRsrc Severity: Critical Log: NE302	Cause: Mate card communication failure Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing an ITX card.
Type: ITXLinkRsrc Severity: Minor Log: NE304	Cause: Link (4-19) [faceplate port (0-7)] to ITP card Action: Two cards cannot communicate with each other. Diagnostics will isolate the fault and determine the course of action. The alarm will change to an NE305 within 3 minutes.
Type: ScLinePortUnstableRsrc Severity: Major Log: NE305	Cause: The rate of Signal State Change Interrupt (SSI) messages on the affected card exceeds a safe operational threshold. Action: If the alarm affects an active card, the alarm causes a SWACT, which changes the state of the card to inactive. Monitor the inactive card for 1 hour. If the alarm occurs on an inactive card, and no further link faults occur, the system clears the alarm automatically after 1 hour. If the system does not clear the alarm on an inactive card after 1 hour, replace the card.
Type: ITXPortRsrc Severity: Minor Log: NE305	Cause: Serial Device (4-19) [faceplate port (0-7)] to ITP card Action: Check the ITP card for alarms. If alarms exist, clear those alarms. If there are no alarms on the ITP card, or only external alarms are on the ITX card, replace the cable between the ITP and the ITX cards. If the alarm is on a DCC card, clear any DCC card alarms. Reseat the ITX card and determine if the alarm clears. Reseat the DCC card and determine if the alarm clears.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITXExternalRsrc Severity: Minor Log: NE305	Cause: External: ITP attached to Serial Device (4-19) [faceplate port (0-7)] Action: Check the ITP card for alarms. If alarms exist, clear those alarms. If there are no alarms on the ITP card, or only external alarms are on the ITX card, replace the cable between the ITP and the ITX cards. If the alarm is on a DCC card, clear any DCC card alarms. Reseat the ITX card and determine if the alarm clears. Reseat the DCC card and determine if the alarm clears.
Type: ITXIntercardRsrc Severity: Minor Log: NE305	Cause: Backplane connection to DCC in slot (10, 11) or Cable attached to Serial Device (4-19) [faceplate port (0-7)] Action: Check the ITP card for alarms. If alarms exist, clear those alarms. If there are no alarms on the ITP card, or only external alarms are on the ITX card, replace the cable between the ITP and the ITX cards. If the alarm is on a DCC card, clear any DCC card alarms. Reseat the ITX card and determine if the alarm clears. Reseat the DCC card and determine if the alarm clears.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITXLineSideGrpRsrc Severity: Major Log: NE305	Cause: Port (0 to 7) to ITP pair Action: This fault is ambiguous with regard to the card that is causing the fault. Usually, the alarm on the ITX indicates that there is a problem on the ITX card, DCC card, or the link in between the DCC card and the ITX card. Try each of the following, until the problem clears: • Restart the ITX card from the current load. • Restart the DCC card from the current load. • Replace ITX card. • Reinstall the old ITX card and replace the DCC card. • Visually inspect the backplane looking for bent or damaged pins.
Type: ITXNetForwarderRsrc Severity: Major Log: NE305	Cause: Net side cell forwarder Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ITX card.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITXcardNEProxy Severity: Major Log: NE318	Cause: ITX card NE proxy. Card communication failure. Proxy mode activated. Action: Perform the following steps: 1. Wait about 2 minutes to see if the alarm clears on its own. The alarm may be caused by a restart or any break in communication that may clear automatically. 2. Check the alarm log report to see if the active C-side path has any faults. If so, follow the alarm clearing procedures for those faults. 3. Lock and offline the card. Unseat the card from the backplane, then reseat it. 4. Repeat step 1. If the alarm does not clear then replace the card. Go to Replacing an ITX card. After replacing the card, repeat step 1. If the alarm still does not clear, call Nortel Networks for support.
Type: ITXLineForwarderRsrc Severity: Major Log: NE305	Cause: Line side cell forwarder Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ITX card.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITXFramerRsrc Severity: Major Log: NE309	Cause: Framer - timing synchronization device Action: If fault is on both ITPs: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card.
Type: ITXNetworkSideIfPortRsrc Severity: Minor Log: NE310 ***Note:*** When this is raised, it most likely is a hardware problem on an unused resource and can be ignored.	Cause: Port 2 on serial device - port only used by diagnostics Action: If fault is on both ITPs: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITXBITSRefRsrc Severity: Minor Log: NE309	Cause: BITS click reference (A or B) Action: If fault is on both ITPs: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card.
Type: CardTypeMismatchRsrc Severity: Critical Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ITX card.
Type: IdpromRsrc Severity: Major Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ITX card.
Type: CardPairOOSRsrc Severity: Warning Log: NE301	Cause: Active/Master Card Out of Service Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ITX card.

ITX card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: RedundancyLostRsrc Severity: Warning Log: NE301	Cause: Simplex Mode - No Redundancy Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ITX card.
Type: ITXCableRsrc Severity: Minor Log: NE312	Cause: Cable configuration conflict, port (0 to 7) Action: One of the cables to the ITPs has been connected in an unsupported way. Check to see if the cable on this ITX matches the mate ITX, and that the ITP ends of the cable are in the right ports.
Type: Atm50PortRsrc Severity: Minor Log: NE301	Cause: ATM200 Port (0-19); Not at 2000 speed or initialization failed Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ITX card.
Type: norNodeSwact Severity: None Log: NE500	Cause: Card has performed a switch of activity (SWACT). Action: None, for information only.
Type: norNodeStateChange Severity: None Log: NE501	Cause: Card has performed a state change. Action: None, for information only.
Type: PatchAlarmFault Severity: Major Log: PATC301	Cause: This alarm is generated when a patch alarm fault is received on an MG 9000 ITX card indicating a restart is required after a patch has been removed or applied. Action: Restart the affected card by performing the procedure Restarting a card on page 348.

Clearing MG 9000 ITP card and VMG alarms

Purpose of this procedure

This section identifies the alarms generated for the ITP card, ITP VMG, and ABI VMG, the alarm severity, the log report, the cause of the alarm, and the recovery methods. ITP alarms are derived from faults detected by the ITP card.

> ***Note:*** For ESA alarms raised on ABI (DS-512) VMGs, the ESA alarms listed in this section also apply.

This section provides clearing information for the following alarms:

- ESA alarms on page 135
- ITP card alarms on page 137
- VMG alarms on page 161

When to use this procedure

Use this procedure when MG 9000 ITP card alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with an ITP fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser.
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appear in the Description field.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
ESA alarms	
Type: EnteredESA Severity: Critical Log: ESA300	Cause: Communication between GWC and MG 9000 is lost. Entered ESA mode. Action: Check communication between the VMG and GWC. Check the service state of the GWC. ***Note:*** If the Core loses connectivity with the ABI VMG for more than 25 s, the VMG and hence the XPM, enters ESA. The XPM becomes System Busy (SysB). Calls warm enter ESA, however ESA warm exit on ABI is not supported and calls drop when the Core completes the restart and resumes connectivity with the ABI and the XPM.
Type: nnESARetrievalFault Severity: Critical Log: ESA301	Cause: Data download of ESA data from the CS 2000 Core has failed. Action: Perform a manual download of ESA data and the alarm will clear. Refer to the “Downloading ESA data” procedure in *MG 9000 Configuration Management*, NN10096-511.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: nnESACOIfault Severity: Major Log: ESA304	Cause: Community of interest (COI) network failure. Internodal ESA will either not function at all or function only partially. ESA functionality should still be available within the MG 9000 network element. This is not service affecting unless the VMG enters ESA mode. Action: Check the failure cause in alarm or log text and perform corrective action. This typically will require network route troubleshooting. The MG 9000 clears the alarm autonomously once the root cause is fixed.
Type: CoreDownloadFailed Severity: Minor Log: ESA311	Cause: Core Download Failed - This alarm is generated by the MG 9000 Manager when a problem is detected when trying to download the data file from the Core. This condition results when the Core data file is more than 48 hours old, indicating that the file on the Core is not being generated nightly. Action: Refer to the alarm text presented in the Alarm Browser for actions based on the condition the caused the alarm.
Type: InternodalESACOIdataFault Severity: Major Log: ESA312	Cause: Generated by the MG 9000 Manager when a failure occurs while trying to provision Internodal community of interest data for a given NE. Action: Check the failure cause in alarm or log text. The most common is communication failure between the MG 9000 Manager and the MG 9000. Once the root cause is fixed, the alarm can be cleared by running an NE audit on the affected MG 9000 or pressing Apply on the Internodal ESA configuration GUI. For information on the NE audit, refer to procedure "Performing an MG 9000 data audit" in *MG 9000 Configuration Management*, NN10096-511.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ESAProvisioningFault Severity: Critical Log: ESA313	Cause: MG 9000 Manager unable to download ESA data to a VMG. Action: Perform a manual download of ESA data and the alarm will clear. Refer to the “Downloading ESA data” procedure in *MG 9000 Configuration Management*, NN10096-511.
ITP card alarms	
Type: ITPGlanHubRsrc Severity: Critical Log: NE306	Cause: GLAN Hub, communicates with other cards on shelf Action: The GLAN hub is located on the active ITP in the shelf where the fault appears. First try performing a SWACT of the ITP cards and re-run diagnostics on the problem card. If that does not fix the problem, replace the newly inactive ITP, otherwise, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPClockSyncRsrc Severity: Critical Log: NE309	Cause: Clock Sync Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: MegacoDataSyncRsrc Severity: Critical Log: NE302	Cause: Megaco Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ATMDataSyncRsrc Severity: Critical Log: NE302	Cause: ATM Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BALDataSyncRsrc Severity: Critical Log: NE302	Cause: BAL Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: NodeSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Node Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BaseSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Base Platform Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: TestSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Test Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ShfSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Shelf Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ClkSyncSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Clock Sync Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MarketFitSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Market Fit Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: MateCommunicationRsrc Severity: Critical Log: NE302	Cause: Mate card communication failure Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: LineSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Line Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: UpgSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Software Upgrade Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ESASubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: ESA Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MegacoSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Megaco Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: MegOmsSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Megaco OMs Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ScLinePortUnstableRsrc Severity: Major Log: NE305	Cause: The rate of Signal State Change Interrupt (SSI) messages on the affected card exceeds a safe operational threshold. Action: If the alarm affects an active card, the alarm causes a SWACT, which changes the state of the card to inactive. Monitor the inactive card for 1 hour. If the alarm occurs on an inactive card, and no further link faults occur, the system clears the alarm automatically after 1 hour. If the system does not clear the alarm on an inactive card after 1 hour, replace the card.
Type: ITPLineSideIfRsrc Severity: Major Log: NE305	Cause: Serial device 0 - to Line Card Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPNetworkIntercardRsrc Severity: Major Log: NE305	Cause: Backplane connection to mate ITP card; cable between ITX and ITP cards on ITP port (0, 1) Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPDspServiceCircuitsRsrc Severity: Major Log: NE301	Cause: Tone generation service, DSP # (0 to 3) Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPAal1SarRsrc Severity: Major Log: NE301	Cause: AAL1 SAR - Call Traffic TDM to ATM converter Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPAtmBusControllerRsrc Severity: Major Log: NE301	Cause: Serial Link Control - controls communication with ITX cards Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPcardNEProxy Severity: Major Log: NE318	Cause: ITP card NE proxy. Card communication failure. Proxy mode activated. Action: Perform the following steps: 1. Wait about 2 minutes to see if the alarm clears on its own. The alarm may be caused by a restart or any break in communication that may clear automatically. 2. Check the alarm log report to see if the active C-side path has any faults. If so, follow the alarm clearing procedures for those faults. If the ITP has proxy faults, check the active ITX card and the active DCC for ATM port faults. If the ITX has a port fault, clear the fault. 3. Verify the cable to the active ITX card is connected. Unplug and replug the cable at the ITP end if necessary. 4. Lock and offline the card. Unseat the card from the backplane, then reseat it. 5. Repeat step 1. If the alarm does not clear then replace the card. Go to Replacing an ITP card. After replacing the card, repeat step 1. If the alarm still does not clear, call Nortel Networks for support.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPDdcIdpromRsrc Severity: Minor Log: NE301	Cause: DSP daughter card Id PROM failure Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPDdcCalistoRsrc Severity: Major Log: NE301	Cause: DSP daughter card Calisto failure Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPVoicePathRsrc Severity: Critical Log: NE301	Cause: DSP (1-4) voice path resource failure. Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: DLMSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Data Line Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: FileDescRsrc Severity: Major Log: NE302	Cause: Startup failure: Data Line Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPDalFaultRsrc Severity: Major Log: NE301	Cause: Hardware failure or a failure to connect individual digital signal processor (DSP) abstraction layer (DAL) channel activation requests. This results in call setup not completing and the user experiencing a drop back to dial tone after dialing the terminating party. Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Market Fit Download Failure Severity: Major Log: N/A	Cause: Market fit download failure occurred. The MG 9000 received bad or unexpected information in the market fit data from the MG 9000 Manager. This fault may be the result of: • a data transmission error in SNMP from the MG 9000 Manager. This will be seen on initial VMG provisioning or when changing the market for a VMG. • bad data in the market configuration files on the MG 9000 Manager. This will be seen on initial VMG provisioning or when changing the market for a VMG. • bad persistence of the market fit data. This would be the case when a pair of ITP cards have restarted. As a result of this error, there is a reduction of complete lack of call processing capability on the MG 9000. The most common symptom is a complete lack or reduction of tones capability. Action: • If the fault was raised on a restart of a pair of ITP cards, check for a fault for Flash on the card. • If the fault was raised on initial VMG provisioning or when changing the market fit for a VMG, it is possible that the data was corrupted when the data was transmitted to the MG 9000. To resolve a transmission error of the market fit data, re-send the market fit data for this market to the MG 9000. To re-send the data, press the Apply button on the GW Market Config tab of the Switched Lines Services GUI for the VMG that has the fault.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPDDCAAL5SARRsrc Severity: Major Log: NE305	Cause: DDC AAL5 SAR - Call traffic TDM to IP converter Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPMateSideExternalRsrc Severity: Major Log: NE304	Cause: Mate ITP Card, or link to Mate Action: This fault is ambiguous with regard to the card that is causing the fault. Usually, the alarm on the ITP indicates that there is a problem on the ITP card, DCC card, or the link in between the DCC card and the ITP card. Try each of the following, until the problem clears: • Restart the ITP card from the current load. • Restart the DCC card from the current load. • Replace ITP card. • Reinstall the old ITP card and replace the DCC card. • Visually inspect the backplane looking for bent or damaged pins.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: DPLL unit on ITP failed or no signal Severity: Major Log: NE309	Cause: Clock Sync: DPLL unit on this ITP failed or no signal Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPClockPhaseLockRsrc Severity: Major Log: NE309	Cause: Clock Sync: Loss of Phase Lock Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPClockFramePulseRsrc Severity: Major Log: NE309	Cause: Clock Sync: Loss of Frame Pulse Lock Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPClockMyClockRsrc Severity: Critical Log: NE309	Cause: Clock Sync: Loss of My Clock Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPTimeswitchRsrc Severity: Major Log: NE301	Cause: Timeswitch - call processing engine Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing an ITP card.
Type: ITPTimeswitchEcanRsrc Severity: Major Log: NE301	Cause: Timeswitch ECAN Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing an ITP card.
Type: ITPCallPBusRsrc Severity: Major Log: NE301	Cause: CallP Bus Interface - bridge between ATM50 and CallP SAR Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing an ITP card.
Type: ITPDdcHeartbeatRsrc Severity: Major Log: NE301	Cause: DDC Heartbeat timer timeout Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing an ITP card.
Type: ITPJanusDspRsrc Severity: Critical Log: NE301	Cause: Janus DSP Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing an ITP card.
Type: ITPSignalingPathRsrc Severity: Major Log: NE301	Cause: Signaling path Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPClockOutputRsrc Severity: Critical Log: NE309	Cause: Clock Sync: Loss of Clock Output Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPSyncAllRefRsrc Severity: Major Log: NE309	Cause: Clock Sync: All Reference Failure Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPSyncSingleSyncRsrc Severity: Major Log: NE309	Cause: Clock Sync: Single Sync Unit Failure Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPClockSyncLostRsrc Severity: Major Log: NE309	Cause: Clock Sync: Loss of Clock Synchronization Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPSyncHORsrc Severity: Minor Log: NE309	Cause: Clock Sync: Holdover Mode Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPWBCallConnRsrc Severity: Major Log: NE302	Cause: Call Control Connection Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: DataMismatchRsrc Severity: Critical Log: NE302	Cause: Data Mismatch with DCC Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPSyncLOSRsrc Severity: Minor Log: NE309	Cause: Clock Sync: Loss of Signal Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPSyncOOFRsrc Severity: Minor Log: NE309	Cause: Clock Sync: Out of Frame Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPSyncHORsrc Severity: Major Log: NE309	Cause: Clock Sync: Holdover Mode Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPCableRsrc Severity: Minor Log: NE312	Cause: Cable configuration conflict Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPClockMateClockRsrc Severity: Minor Log: NE309	Cause: Clock Sync: Loss of Mate Clock Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: ITPLineSideExternalRsrc Severity: Minor Log: NE304	Cause: Line Card 0, or link to Line Card Action: Two cards cannot communicate with each other. Diagnostics will isolate the fault and determine the course of action. The alarm will change to an NE305 within 3 minutes.
Type: ITPNetworkLinkRsrc Severity: Minor Log: NE304	Cause: Link to ITX, port (0 to 1) - isolation in progress, Link to Mate ITP Action: Two cards cannot communicate with each other. Diagnostics will isolate the fault and determine the course of action. The alarm will change to an NE305 within 3 minutes.
Type: ITPNetworkExternalRsrc Severity: Minor Log: NE304	Cause: External: Mate ITP; External: ITX attached to port (0, 1) Action: Check the ITX to see if it has alarms. If so, clear the alarms first. If no alarms are on the ITX card, or only External alarms are on the ITX card, replace the cable between the ITX and the ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPEchoCancellationRsrc Severity: Minor Log: NE301	Cause: ECAN module Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPSyncSingleRefRsrc Severity: Minor Log: NE309	Cause: Clock Sync: Single Reference Failure Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: CardTypeMismatchRsrc Severity: Critical Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: IdpromRsrc Severity: Major Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: CardPairOOSRsrc Severity: Warning Log: NE301	Cause: Active/Master Card Out of Service Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: RedundancyLostRsrc Severity: Warning Log: NE301	Cause: Simplex Mode - No Redundancy Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ITP card.
Type: ITPClockRsrc Severity: Variable Log: NE309	Cause: Clock Sync: Clock Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: TestRsrc Severity: variable Log: NE302	Cause: Test Resource Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ITPSyncRsrc Severity: Variable Log: NE309	Cause: Clock Sync: Sync Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: Large number of call processing failures in the network element Severity: NA (may not appear as a single fault at the alarm browser) Log: None	Cause: The active ITP card in the active shelf provides timing signals for the other cards in the master shelf. A large number of call processing failures in the network element may point to a failure in the active ITP card. Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults persist, replace the card. Go to Replacing an ITP card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Downstream FIFO Severity: Major Log: NE316	Cause: ADSL: Downstream FIFO. Indicates the ATM50 FIFO buffer, which handles ADSL data transfer is being overrun with cells from the network. When the alarm is raised, back pressure is also asserted which tells the DCC OC-3 card of the condition and causes it to back off or stop the data transfer. Action: The alarm clears after the condition is alleviated, back pressure is removed, and data flow continues. To manually clear the alarm, lock and unlock the data circuit. Go to the Locking a voice or data line circuit and Unlocking a voice or data line circuit procedures.
Type: Downstream HEC Severity: Major Log: NE316	Cause: ADSL: Downstream ATM50 Header Error Control (HEC) problem Action: Since this problem is associated with the data side of the card only, a warm restart of the ADSL card will clear the data side problem without affect the voice side. Perform a warm restart of the ADSL line card. Refer to Restarting a card.
Type: ATM50Fault Severity: Critical Log: NE316	Cause: ADSL: ATM50 fault Action: Restart the ADSL line card. Refer to Restarting a card.
Type: Upstream buffer overflow Severity: Critical Log: NE316	Cause: ADSL: Upstream buffer overflow Action: Throttle back the upstream data rate to the line card
Type: ATM device timeout Severity: Critical Log: NE316	Cause: ADSL: ATM device timeout Action: Throttle back the downstream data on the line card.
Type: Clock accuracy Severity: Critical Log: NE316	Cause: ADSL: Loss of clock accuracy Action: Restart the ADSL line card. Refer to Restarting a card.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: DSP lockup Severity: Critical Log: NE316	Cause: ADSL: DSP lockup Action: Restart the ADSL line card. Refer to Restarting a card.
Type: norNodeSwact Severity: None Log: NE500	Cause: Card has performed a switch of activity (SWACT). Action: None, for information only.
Type: norNodeStateChange Severity: None Log: NE501	Cause: Card has performed a state change. Action: None, for information only.
Type: ovldDetectionAlarm Severity: Minor/Major Log: OVLD304	Cause: This alarm is generated when an overload detection alarm is received from an MG 9000. Indicates a performance trouble has occurred. Action: Calls may be lost. Check the resource usage for this network element.
Type: ovldRscMonPduRateFault Severity: Warning Log: OVLD800	Cause: This alarm is generated when an Pdu rate overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: ovldRscMonCbvMsgRFault Severity: Warning Log: OVLD801	Cause: This alarm is generated when an Cbv message rate overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: ovldRscMonConnQueFault Severity: Warning Log: OVLD802	Cause: This alarm is generated when an connection queue overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ovldRscMonCpuUtilFault Severity: Warning Log: OVLD803	Cause: This alarm is generated when an CPU utilization fault is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: perfMonCpuFault Severity: Warning Log: OVLD804	Cause: This alarm is generated when a CPU utilization overloaded alarm is received from an MG 9000. Action: None, for information only.
Type: perfMonRamFault Severity: Warning Log: OVLD805	Cause: This alarm is generated when a PM RAM utilization fault is received from an MG 9000. Action: None, for information only.
Type: perfMonFlashFault Severity: Warning Log: OVLD806	Cause: This alarm is generated when a PM flash utilization fault is received from an MG 9000. Action: None, for information only.
Type: perfMonChannFault Severity: Warning Log: OVLD807	Cause: This alarm is generated when a PM channel utilization fault is received from an MG 9000. Action: None, for information only.
Type: PatchAlarmFault Severity: Major Log: PATC301	Cause: This alarm is generated when a patch alarm fault is received on an MG 9000 ITP card indicating a restart is required after a patch has been removed or applied. Action: Restart the affected card by performing the procedure Restarting a card on page 348.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
VMG alarms	
Type: VMG OOS Severity: Critical Log: VMG300	Cause: Root termination has gone out of service (communication between the MG 9000 and the GWC is lost and ESA is not enabled). Action: Using the Traceroute or Ping MG9000 tool, test the network communication path between the MG 9000 Manager and the MG 9000. Check the OC-3 connection at the MG 9000. Check the state of the cards in the MG 9000, including the ABI or ITP cards for this VMG, the DCCs, and for the case of ITP cards, the ITX cards. Verify that the Admin Status of the VMG is 'In Service'. Check the service state of the GWC. Correct any problems found. This alarm is raised only for transient situations, and should either be cleared or replaced by a different alarm within 15 seconds. The two exceptions to this are: • the active card is at SN07 or greater, but the inactive card is on a pre-SN07 software release • the ITP or ABI pair is on SN07, but the DCC is on a pre-SN07 release Until the inactive card and DCC are upgraded to SN07 or greater, the active card will raise only the VMG300 fault when the VMG is out of service. To clear this, follow the instructions for the various faults until the alarm is cleared. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm SWACT of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: BadCalls Severity: MInor Log: VMG301	Cause: QoS alarm generated when the number of bad calls reaches a certain threshold Action: Check the GWC QOS collector for any QOS errors. Narrow down possible problem by running test calls. If the error is only on that one line, there may be a card fault. If problem is in the network, isolate the problem area and correct.
Type: PacketLoss Severity: Minor Log: VMG302	Cause: QoS alarm that is generated when the number of Packets lost reaches a certain threshold Action: Check the GWC QOS collector for any QOS errors. Narrow down possible problem by running test calls. If the error is only on that one line, there may be a card fault. If problem is in the network, isolate the problem area and correct.
Type: Jitter Severity: Minor Log: VMG303	Cause: QoS alarm that is generated when IP message jitter reaches a certain threshold. Action: Check the GWC QOS collector for any QOS errors. Narrow down possible problem by running test calls. If the error is only on that one line, there may be a card fault. If problem is in the network, isolate the problem area and correct.
Type: Latency Severity: Minor Log: VMG304	Cause: QoS alarm that is generated when IP message latency reaches a certain threshold. Action: Check the GWC QOS collector for any QOS errors. Narrow down possible problem by running test calls. If the error is only on that one line, there may be a card fault. If problem is in the network, isolate the problem area and correct.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ALFalarm Severity: Major Log: VMG311	Cause: Application layer framing (ALF) alarm occurs when the MG 9000 is experiencing Megaco retransmissions greater than 50% for a period of 5 minutes or more. This means that over 50% of the messages sent to the GWC by the MG 9000 are retransmissions of an earlier message. Action: Verify the MG 9000 is in service from the GWC perspective. Check the network connection between the GWC and the MG 9000.
Type: Megaco Task alarm Severity: Major Log: VMG312	Cause: Megaco task alarm indicates one or more of the Megaco Task's input buffers are over 90% full for a period of 5 minutes or more. This means this Megaco Talk input source is not being processed by Megaco in a timely manner or that the source is being bombarded by an external entity. For example, if the line card input source is full this could indicate that a line card is babbling so fast that Megaco cannot process all the messages and thus the input pipe is backing up. Currently, the Megco Task has input sources: line card, DSP, GWC, datasync, OAMP, Audits, ESA, ABI DSP, CES, and timers. The task alarm can be raised for any of these input sources or for a combination of these sources. Action: Check the following based on the input source: • line card - indicates the MG 9000 has a babbling line card. All line cards should be checked. • DSP - indicates the MG 9000 has a babbling DSP. If the alarm is not raised on the inactive ITP card, perform a SWACT of the ITP card. • GWC - indicates the GWC is flooding the MG 9000 with messages. Check the GWC for faults. • datasync - indicates the active ITP card is flooding the inactive ITP card with messages.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Megaco Task alarm (Contd)	Action: (Contd) • OAMP - indicates the MG 9000 Manager is flooding the MG 9000 with messages. Check the MG 9000 Manager for faults. • audits - indicates an ITP internal audit has failed. • ESA - indicates the ESA task is flooding the Megaco CallP Task with messages. • ABI DSP - indicates the ABI card is flooding the ITP card with messages • CES - indicates the DCC card is flooding the ITP and/or the ABI cards with messages. • timers - indicates some timer has failed.
Type: Megaco Fault alarm Severity: Major Log: VMG313	Cause: Equipment malfunction due to DSP resource overload. Action: No action required. During the alarm state, new requests are diverted from the overloaded DSP to the other DSPs until the overloaded DSP recovers from the overload condition.
Type: VMGAdminStatusOutOfService Severity: Warning Log: VMG322	Cause: VMG Administrative State Out Of Service - Call Processing Out of Services Action: Change the Administrative status in the Gateway Status Config tab of the Switched Lines Services GUI to In Service. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm SWACT of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: VMGOOSCardLocked Severity: Warning Log: VMG323	Cause: Card Locked - Call Processing Out of Services Action: Unlock the active ITP or ABI card. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm SWACT of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.
Type: VMGOOSCardDisabled Severity: Critical Log: VMG324	Cause: Card Disabled - Call Processing Out of Service. This alarm indicates the ITP or ABI card's status is disabled. Action: The ITP or ABI card view or Alarm Browser will provide more information about what is preventing the card from going enabled. When the card's status goes to enabled, this alarm will be cleared. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: VMGInitializing Severity: Warning Log: VMG325	Cause: VMG Initializing - Call Processing Out of Service. This alarm is raised at initial VMG creation, while waiting for a reply from the GWC when the VMG Admin status is changed to InService or as the active ABI/ITP is coming up out of a restart. Action: There is no clearing procedure for this alarm. During a restart, this is raised as long as 15 minutes. During the first 15 minutes after a restart of an ITP pair, no other out of service VMG alarms are raised against the VMG, except the Card Locked and Admin State Out of Service faults. If the VMG is still Out of Service 15 minutes after the restart, the alarm will be cleared and replaced by the appropriate VMG fault indicating the fault condition at that time. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.
Type: vmgOOSLineMtcNotReady Severity: Critical Log: VMG328	Cause: Line Maintenance Not Ready - Call Processing Out of Service. This alarm indicates Line Maintenance on the ITP or ABI is not ready for call processing support. Action: If this is raised when the card is enabled, then this is likely a software error condition. If the ITP or ABI card is disabled, the Line Maintenance fault is raised as well. Lock and unlock the affected card to clear the alarm. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: vmgOOSMegacoMtcNotReady Severity: Critical Log: VMG329	Cause: Megaco Maintenance Not Ready - Call Processing Out of Service. This fault would be raised because of a software error condition. Action: Lock and unlock the affected card to clear the alarm. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: vmgOOSGWCUnreachable Severity: Critical Log: VMG373	Cause: GWC Unreachable - Call Processing Out of Service. This alarm indicates the GWC is not responding to pings from the ITP or ABI and either the VMG has never reached an Enabled state or ESA capability is not turned on for this VMG. Action: This alarm may mean • the VMG has never been in service, it could be because an invalid VMG IP address was provisioned. If the address is incorrect, then delete and re-add the VMG with the correct IP address. • a problem exists with the network interface or edge router, most likely there will also be a Wanbuilder Heartbeat alarm. Resolve that alarm. • there is not a Wanbuilder Heartbeat alarm and Wanbuilder Heartbeat was turned on for the Call Control subnet (ITPs) or ABI subnet (ABIs), which is likely a network issue. Perform pings/traceroutes to further isolate the problem. • the active GWC is locked and does not respond to pings. Verify that the pair of GWC cards is unlocked. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: vmgOOSNoReplyFromGWC Severity: Critical Log: VMG374	Cause: GWC Reachable But No Reply To Service Change - Check LGRP/GWC state - Call Processing Out of Services. This alarm indicates the GWC is not responding to Megaco messages for this VMG and either the VMG has never reached an Enabled state or ESA capability is not turned on for this VMG. Action: This alarm may mean • the LGRP for this VMG is not in a ready state. Check the LGRP state using MAPCI; PM on the Core. • this is a VMG for an ABI pair that has never been in service. This could mean that the Core or MG 9000 Manager is provisioned with the incorrect address for this VMG. Correct the VMG IP address in the datafill in the core or re-provision the VMG with the correct address in the MG 9000 Manager. • the GWC pair has been set to man busy or has problems. Check the GWC status in CS 2000 Management Tools. ***Note 1:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344. ***Note 2:*** If the Call Control Heartbeat fault is raised for this NE, the GWC is usually not reachable. However, in SN07 if the call control heartbeat address is not reachable (consequently, the call control heartbeat fault is raised) and the VMG is out of service, the VMG374 fault is raised instead of the fault that should be raised, which is the VMG373 (vmgOOSGWCUnreachable) fault.

ITP and VMG card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: vmgOOSAAL1BearerSubsystemOnPairNotReady Severity: Critical Log: VMG376	Cause: AAL1 Bearer Not Ready - Call Processing Out of Service. Action: This indicates a software error on either the DCC or ITP card. Lock and unlock the ITP, ABI, or DCC card(s) to clear this alarm. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.
Type: vmgOOSIPBearerSubsystemOnPairNotReady Severity: Critical Log: VMG377	Cause: IP Bearer Not Ready - Call Processing Out of Service. Action: This may indicate the Call Control Subnet was not provisioned on the DCC. Go to LCI and provision the Call Control Subnet. If the Call Control Subnet has been provisioned and this fault does not clear, this is likely a software error. Lock and unlock the affected ITP or ABI card. ***Note:*** In rare circumstances, a VMG alarm could fail to clear even though call processing is in service. If this occurs, perform a warm swact of the ITP or ABI card pair to clear the fault. Refer to Switching activity of a card on page 344.
Type: Databaseunavailable Severity: Warning Log: VMG600	Cause: Termination data was successfully provisioned in all appropriate except for the databases. Action: None, for information only. The database will be corrected when it is available.
Type: Databasecorrected Severity: Warning Log: VMG601	Cause: An attempt to correct termination data in the database has passed. Action: None, for information only.

Clearing MG 9000 clock sync alarms

Purpose of this procedure

This procedure identifies the alarms generated for clock sync at the ITP card, the alarm severity, the log report, the cause of the alarm, and the recovery methods. Clock sync alarms are derived from faults detected by the ITP card.

When to use this procedure

Use this procedure when MG 9000 ITP card clock sync alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

The faults indicated in the following table should be correlated with a clock sync fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser.
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appear in the Description field.

Clock sync alarms

Alarm type, severity, and log report	Cause and action
Type: lossOfPhaseLock Severity: Minor Log: CLK301	Cause: The inactive ITP card’s sync unit will not lock to the active ITP card’s sync unit Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

Clock sync alarms

Alarm type, severity, and log report	Cause and action
Type: signalLof Severity: Major Log: CLK313	Cause: Loss of frame. This fault has no alarms, though a failure on the timing signal will probably result in a reference failure. Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

Clock sync alarms

Alarm type, severity, and log report	Cause and action
Type: lossOfFramePulseLock Severity: Major Log: CLK302	Cause: Frame pulses between the ITPs do not match. Each ITP card generates its own alarm. Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: lossOfMyClock Severity: Major Log: CLK303	Cause: Sync unit on one of the ITP cards failed Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

Clock sync alarms

Alarm type, severity, and log report	Cause and action
Type: lossOfMateClock Severity: Major Log: CLK304	Cause: Sync unit on one of the ITP cards failed Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: lossOfClockOutput Severity: Major Log: CLK305	Cause: The ITP is not generating a 20.48 clock output signal. Both ITPs are not generating a 20.48 clock output signal Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

Clock sync alarms

Alarm type, severity, and log report	Cause and action
Type: allReferenceFailure Severity: Major Log: CLK307	Cause: Both absolute and delta referenced source signals have failed Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.
Type: singleSyncUnitFailure Severity: Major Log: CLK308	Cause: Stratum 3 unit on ITP card failed Action: If fault is on both ITP cards: 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

Clock sync alarms

Alarm type, severity, and log report	Cause and action
Type: signalLos Severity: Major Log: CLK312	Cause: Loss of signal. This fault has no alarms, though a failure on the timing signal will probably result in a reference failure. Action: If fault is on both ITP cards 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

Clock sync alarms

Alarm type, severity, and log report	Cause and action
Type: singleReferenceFailure Severity: Minor Log: CLK306	Cause: Provisioned reference is in the failed state Action: If fault is on both ITP cards 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. If fault persists, call next level of support. If fault is on one ITP card 1. Verify Clock source is connected. 2. Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3. If fault persists, lock/unlock to restart the card. 4. Replace the faulty card. Go to Replacing an ITP card.

Clearing MG 9000 DS1 card alarms

Purpose of this procedure

This procedure identifies the alarms generated for the DS1 card, the alarm severity, the log report, the cause of the alarm, and the recovery methods. DS1 alarms are derived from faults detected by the DS1 card.

When to use this procedure

Use this procedure when MG 9000 DS1 card alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a DS1 fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser.
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appear in the Description field.

Note: If the attempt to clear the alarm fails, please contact your next level of support.

DS1 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: DS1UtopiaBridgeRsrc Severity: Major Log: NE305	Cause: Utopia Bus Master - AAL1, AAL5 to ATM PHYs Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: DS1FramerRsrc Severity: Major Log: NE301	Cause: DS1 Framer for DS1 links (0-7 or 8-15) Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: DS1cardNEProxy Severity: Major Log: NE318	Cause: DS1 card NE proxy. Card communication failure. Proxy mode activated. Action: Perform the following steps: 1. Wait a about 2 minutes to see if the alarm clears on its own. The alarm may be caused by a restart or any break in communication that may clear automatically. 2. Check the alarm log report to see if the active C-side path has any faults. If so, follow the alarm clearing procedures for those faults. 3. Lock and offline the card. Unseat the card from the backplane, then reseat it. 4. Repeat step 1. If the alarm does not clear then replace the card. Go to Replacing a DS1 card. After replacing the card, repeat step 1. If the alarm still does not clear, call Nortel Networks for support.

DS1 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: DS1NetworkPortlRsrc Severity: Minor Log: NE304	Cause: Serial Device (0, 1) to DCC card in slot (10, 11) Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: DS1NetworkExternalRsrc Severity: Minor Log: NE305	Cause: External: DCC Card in slot (10 or 11) Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: DS1NetworkIntercardRsrc Severity: Minor Log: NE305	Cause: Backplane connector to DCC Card in slot (10 or 11) Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: DS1NetworkLinkRsrc Severity: Minor Log: NE304	Cause: Link to DCC Card in slot (10 or 11) Action: Two cards cannot communicate with each other. Diagnostics will isolate the fault and determine the course of action. The alarm will change to an NE305 within 3 minutes.
Type: DS1Aal1SarRsrc Severity: Minor Log: NE301	Cause: AAL1 SAR - DS1 Card TDM to ATM converter Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.

DS1 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: DS1LinkRsrc Severity: Minor Log: NE301	Cause: DS1 Link (0 to 15) Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: DS1LIURsrc Severity: Major Log: NE301	Cause: DS1 Line Interface unit for DS1 links (0-7 or 8-15) Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: AtmDataSyncRsrc Severity: Critical Log: NE302	Cause: ATM Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BalDataSyncRsrc Severity: Critical Log: NE302	Cause: BAL Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MegacoDataSyncRsrc Severity: Critical Log: NE302	Cause: Megaco Data Sync. Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BaseSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Base Platform Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: CarmSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Carrier Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

DS1 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: NodeSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Node Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: TestSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Test Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: UpgSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Software Upgrade. Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: DataMismatchRsrc Severity: Critical Log: NE302	Cause: Data Mismatch with DCC Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: FileDescRsrc Severity: Major Log: NE302	Cause: File Descriptors Low Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: TestRsrc Severity: variable Log: NE302	Cause: Test Resource Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: CardTypeMismatchRsrc Severity: Critical Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DS1 card.

DS1 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: CardPairOOSRsrc Severity: Warning Log: NE301	Cause: Active/Master Card Out of Service Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: IdpromRsrc Severity: Major Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: RedundancyLostRsrc Severity: Warning Log: NE301	Cause: Simplex Mode - No Redundancy Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing a DS1 card.
Type: PatchAlarmFault Severity: Major Log: PATC301	Cause: This alarm is generated when a patch alarm fault is received on an MG 9000 DS1 card indicating a restart is required after a patch has been removed or applied. Action: Restart the affected card by performing the procedure Restarting a card on page 348.
Type: ScLinePortUnstableRsrc Severity: Major Log: NE305	Cause: The rate of Signal State Change Interrupt (SSI) messages on the affected card exceeds a safe operational threshold. Action: If the alarm affects an active card, the alarm causes a SWACT, which changes the state of the card to inactive. Monitor the inactive card for 1 hour. If the alarm occurs on an inactive card, and no further link faults occur, the system clears the alarm automatically after 1 hour. If the system does not clear the alarm on an inactive card after 1 hour, replace the card.

Clearing MG 9000 DS-512 card alarms

Purpose of this procedure

This procedure identifies the alarms generated for the DS-512 card, the alarm severity, the log report, the cause of the alarm, and the recovery methods. DS-512 alarms are derived from faults detected by the DS-512 card.

Note: For ESA alarms raised on ABI (DS-512) VMGs, refer to the ESA alarms in the Clearing MG 9000 ITP card and VMG alarms on page 134.

When to use this procedure

Use this procedure when MG 9000 DS-512 card alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a DS-512 fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser.
2. Look at the Description field of the Alarm Browser. The "Cause of alarm" column in the following table corresponds to the text that appear in the Description field.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: A2:ABI/ITP Frame Pulses don't match Severity: Major Log: CLKR643	Cause: A2:ABI/ITP Frame Pulses don't match. An error exists in the timing chain from the ITP through the ABI. This condition could be caused by the ITP or the ABI. If this alarm exists on both paired ABI then the condition is caused by the ITP. If this alarm occurs on a single card then the issue likely exists only on the affected ABI card. Action: This alarm should clear within a few seconds, if this alarm is in a steady alarm condition then it indicates that the ITPs or ABI card should be replaced. If a burst of these alarms appear, contact Nortel.
Type: A1:ABI PLL is out of lock Severity: Major Log: CLKR643	Cause: A1:ABI PLL is out of lock. The PLL on the ABI was unable to lock onto the incoming ITP clock signal. This could be caused by a fault on the ABI or because the ITP's output frequency is beyond the lock range of the ABI PLL. Action: If this alarm exists on both paired ABI cards, the condition is caused by the ITP card. If this alarm occurs on a single ABI card, the issue likely exists only on the affected ABI card. This alarm should clear within a few seconds, if this alarm is in a steady alarm condition then it indicates that the ITPs or ABI card should be replaced.If a burst of these alarms appear, contact Nortel.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: A6:Lost Slot 12 ITP input clock – Simplex timing reference Severity: Minor Log: CLKR643	Cause: A6:Lost Slot 12 ITP input clock – Simplex timing reference. The ABI card has detected a loss of the input clock from the ITP card in slot 12 and the ABI card only has a simplex source (ITP card in slot 13) for its timing reference. Action: This alarm should only occur during brief periods of maintenance actions and should clear on it own. If this alarm is in a steady alarm condition then it indicates that the indicated ITP card should be replaced.
Type: A6:Lost Slot 13 ITP input clock – Simplex timing reference Severity: Minor Log: CLKR643	Cause: A6:Lost Slot 13 ITP input clock – Simplex timing reference. The ABI card has detected a loss of the input clock from the ITP card in slot 13 and the ABI card only has a simplex source (ITP card in slot 12) for its timing reference. Action: This alarm should only occur during brief periods of maintenance actions and should clear on it own. If this alarm is in a steady alarm condition then it indicates that the indicated ITP card should be replaced.
Type: A6:Lost both ITP input clocks – No timing reference Severity: Major Log: CLKR643	Cause: A6:Lost both ITP input clocks – No timing reference. The ABI has detected a loss of the input clock from both ITP cards. It means the ABI card has no timing reference. Action: A SWACT is not performed because under this condition it is not clear that performing a SWACT will improve system performance and may make it worse. If this alarm occurs it indicates that both ITPs in the shelf are having clock issues and immediate analysis into the ITP alarms should be undertaken. If a burst of these alarms appear, contact Nortel.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: A3:Output of ABI clock has been lost Severity: Major Log: CLKR643	Cause: A3:Output of ABI clock has been lost. The ABI card is no longer providing an output clock. Action: The onboard circuitry is no longer properly timed and the data/message path is not operational. This card has failed and should be replaced as soon as possible. Go to Replacing an ABI card.
Type: FlashRsrc Severity: Major Log: NE301	Cause: Flash Memory Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: Aal5SarRsrc Severity: Major Log: NE305	Cause: AAL5-SAR, Messaging Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: GlanRsrc Severity: Minor Log: NE306	Cause: GLAN Link to hub on Active ITP card Action: The GLAN hub is located on the active ITP in the shelf where the fault appears. First try SWACTing the ITP cards and re-run diagnostics on the problem card. If that does not fix the problem, replace the newly inactive ITP, otherwise, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: ProcessorRsrc Severity: Major Log: NE301	Cause: Processor Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ABI card.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: RamRsrc Severity: Major Log: NE301	Cause: RAM Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: MateCommunicationRsrc Severity: Critical Log: NE302	Cause: Mate card communication failure Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics.If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: AtmDataSyncRsrc Severity: Critical Log: NE302	Cause: ATM Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BalDataSyncRsrc Severity: Critical Log: NE302	Cause: BAL Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MegacoDataSyncRsrc Severity: Critical Log: NE302	Cause: Megaco Data Sync Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: BaseSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Base Platform Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: NodeSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Node Maintenance Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: TestSubsytemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Test Mib Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: TestRsrc Severity: variable Log: NE302	Cause: Test Resource Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MegacoSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Megaco Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: MegOmsSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Megaco OMs Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: UpgSubsystemRsrc Severity: Critical Log: NE302	Cause: Startup failure: Software Upgrade Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: DataMismatchRsrc Severity: Critical Log: NE302	Cause: Data Mismatch with DCC Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABIcardNEProxy Severity: Major Log: NE318	Cause: ABI card NE proxy. Card communication failure. Proxy mode activated. Action: Perform the following steps: 1. Wait about 2 minutes to see if the alarm clears on its own. The alarm may be caused by a restart or any break in communication that may clear automatically. 2. Check the alarm log report to see if the active C-side path has any faults. If so, follow the alarm clearing procedures for those faults. 3. Lock and offline the card. Unseat the card from the backplane, then reseat it. 4. Repeat step 1. If the alarm does not clear then replace the card. Go to Replacing an ABI card. After replacing the card, repeat step 1. If the alarm still does not clear, call Nortel Networks for support. ***Note:*** When replacing the DS-512 card in response to this communication fault, a message box will appear when opening the DS-512 Card View. The message instructs the technician to open the Alarm Browser, and look for the proxy alarm for the faulty card. If present, the card is not communicating and the Safe to Pull LED may not light after the card is locked and set Offline. In this scenario, pulling the cards should not introduce any problems to the system.
Type: ABINetworkPortRsrc Severity: Minor Log: NE305	Cause: Serial device (0, 1) - to DCC cards in slot (10, 11) Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABINetworkIntercardRsrc Severity: Minor Log: NE305	Cause: Backplane connection to DCC cards in slot (10, 11) Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: ABIVoicePathRsrc Severity: Critical Log: NE301	Cause: Voice Path Action: If this fault appears in conjunction with external faults, deal with the external faults first. If this fault appears alone, treat it as a card fault. Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: ABINetworkLinkRsrc Severity: Minor Log: NE304	Cause: Link to DCC card in slot (10, 11) - isolation in progress Action: Two cards cannot communicate with each other. Diagnostics will isolate the fault and determine the course of action. The alarm will change to an NE305 within 3 minutes.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABINetworkSideGrpRsrc Severity: Critical Log: NE305	Cause: Both links to DCC card Action: This fault is ambiguous with regard to the card that is causing the fault. Usually, the alarm on the DCC indicates that there is a problem on the DCC card, ABI card, or the link in between the DCC card and the ABI card. Try each of the following, until the problem clears: • Restart the ABI card from the current load. • Restart the DCC card from the current load. • Replace ABI card. • Reinstall the old ABI card and replace the DCC card. • Visually inspect the backplane looking for bent or damaged pins.
Type: ABILineSideIfRsrc Severity: Major Log: NE307	Cause: DS-512 port Action: Perform the following: • Verify the MG 9000 is in service. • Verify this ABI card is unlocked. • Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. • Check the DS-512 fiber cables (perform a light check, clean fibers, verify fibers are present).
Type: ABILineSideExternalRsrc Severity: Minor Log: NE307	Cause: XPM unit or DS-512 connection Action: Perform the following: • Verify the MG 9000 is in service. • Verify this ABI card is unlocked. • Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. • Check the DS-512 fiber cables (perform a light check, clean fibers, verify fibers are present).

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABITimeswitchNetSideRsrc Severity: Major Log: NE301	Cause: Timeswitch - Call processing engine (network side) Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ABITimeswitchLineSideRsrc Severity: Major Log: NE301	Cause: Timeswitch - Call processing engine (line side) Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ABITimeswitchRsrc Severity: Major Log: NE301	Cause: Timeswitch - Call processing engine Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ABIEchoCancellationRsrc Severity: Minor Log: NE301	Cause: ECAN module - unit (0, 1) Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ABITimeswitchEcanRsrc Severity: Minor Log: NE301	Cause: Timeswitch ECAN unit (key) Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABIFrameSyncRsrc Severity: Warning Log: NE307	Cause: DS512 Framing Manually Overridden - Require Card Restart Action: Perform the following: • Verify the MG 9000 is in service. • Verify this ABI card is unlocked. • Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. • Check the DS-512 fiber cables (perform a light check, clean fibers, verify fibers are present).
Type: ABIAal1SarRsrc Severity: Major Log: NE301	Cause: AAL1 SAR - Call traffic TDM to ATM converter Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ABIAal1NetSideRsrc Severity: Major Log: NE301	Cause: AAL1 Network side unit (0, 1) Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ABIAal1LineSideRsrc Severity: Major Log: NE301	Cause: AAL1 line side unit (0, 1) Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
Type: ABIAtmBusControllerRsrc Severity: Major Log: NE301	Cause: Serial Link Control - controls communication with ITX cards Action: If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABIActivityCableRsrc Severity: Minor Log: NE313	Cause: Activity control cable between ABI cards Action: The activity control cable is a small cable on the front of the ABI cards that is used for activity determination. Perform the following: • Verify the cable is attached to both cards. • Replace cable. • If the fault persists, replace the inactive card. • If the problem still persists, SWACT, replace newly inactive card. Go to Replacing an ABI card.
Type: ABILkmAllChnlsRsrc Severity: Major Log: NE307	Cause: All DS-512 channels closed Action: Perform the following: • Verify the MG 9000 is in service. • Verify this ABI card is unlocked. • Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. • Check the DS-512 fiber cables (perform a light check, clean fibers, verify fibers are present).
Type: ABIWBCallConnRsrc Severity: Major Log: NE302	Cause: Call control connection Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear. Go to Replacing an ABI card.
Type: FileDescRsrc Severity: Major Log: NE302	Cause: File Descriptors Low Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear. Go to Replacing an ABI card.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: CardTypeMismatchRsrc Severity: Critical Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ABI card.
Type: ABIJanusDspRsrc Severity: Critical Log: NE301	Cause: Janus DSP Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card. Go to Replacing an ABI card.
Type: ABIDalFaultRsrc Severity: Major Log: NE301	Cause: Hardware failure or a failure to connect individual digital signal processor (DSP) abstraction layer (DAL) channel activation requests. This results in call setup not completing and the user experiencing a drop back to dial tone after dialing the terminating party. Action: Lock/Unlock the card and the card will restart, most likely causing the alarm to clear. Wait to make sure that the card goes enabled after the restart and no faults re-appear. If the fault re-appears, replace the card. Go to Replacing an ABI card.
Type: CardPairOOSRsrc Severity: Warning Log: NE301	Cause: Active/Master Card Out of Service Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: IdpromRsrc Severity: Major Log: NE301	Cause: Incorrect card in slot Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: RedundancyLostRsrc Severity: Warning Log: NE301	Cause: Simplex Mode - No Redundancy Action: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, replace the card. Go to Replacing an ABI card.
Type: ABIESARecoveryRsrc Severity: Major Log: NE307	Cause: Failed to exit ESA Action: Perform the following: • Verify the MG 9000 is in service. • Verify this ABI card is unlocked. • Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. • Check the DS-512 fiber cables (perform a light check, clean fibers, verify fibers are present).
Type: ScLinePortUnstableRsrc Severity: Major Log: NE305	Cause: The rate of Signal State Change Interrupt (SSI) messages on the affected card exceeds a safe operational threshold. Action: If the alarm affects an active card, the alarm causes a SWACT, which changes the state of the card to inactive. Monitor the inactive card for 1 hour. If the alarm occurs on an inactive card, and no further link faults occur, the system clears the alarm automatically after 1 hour. If the system does not clear the alarm on an inactive card after 1 hour, replace the card.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABI SCTP Message link: failed Severity: Critical Log: OVLD808	Cause: An external messaging link has closed and cannot send/receive messages. The messaging links between the ABI card associated with the XPM and the Gateway Controller (GWC) which the XPM subtends have gone down. This causes a service outage of the XPM and all its subtending peripherals (Emergency Standalone [ESA] may be in effect) Action: Isolate the network components with the problem. If the problem is a transitory problem in a network component, the messaging links may recover autonomously. Any network component used in the messaging path could cause a messaging disruption. Determine if the following components are operating normally: • DS-512 (ABI) card failed or was pulled and not taken out of service first • DCC cards were taken out of service • active DCC card failed or was pulled and not taken out of service The alarm is cleared when the message link is re-established, or by performing maintenance activity at the XA-Core.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABI SCTP Message link: severely degraded Severity: Major Log: OVLD809	Cause: External packet network reliable messaging link(s) severely degraded. Message loss is high enough such that the message link is in a degraded service state. For ABI, this means that some calls are failing and perhaps maintenance actions are failing (such as, static data download). Action: Isolate the network component with the problem. If the problem is transitory in a network component, the messaging links may recover autonomously. Any network component used in the messaging path could cause a messaging disruption. Determine if the following components are operating normally: • DS-512 (ABI) cards in overload • DCC cards in overload The alarm clears when the message link message loss decreases, the critical alarm is raised or by performing maintenance activity from the XA-Core.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ABI SCTP Message link: degraded Severity: Minor Log: OVLD810	Cause: External packet network reliable messaging link(s) degraded. Message retransmissions are high enough that the system is starting to see performance degradation. This may result in increased latency, reduced messaging through the system, buffer overflows, and perhaps congestion. The problem is between the DS-512 cards hosting the XPM and the GWC which the XPM subtends. Messages are being lost, but the system is able to recover with message retransmissions. However, if this situation continues, eventually unrecoverable message loss will occur. Action: Isolate the network component with the problem. If the problem is transitory in a network component, the messaging links may recover autonomously. Any network component used in the messaging path could cause a messaging disruption. Determine if the following components are operating normally: • DS-512 (ABI) cards in overload • DCC cards in overload The alarm clears when the message link message loss decreases, the critical alarm is raised, or by performing maintenance activity from the XA-Core.
Type: ovldDetectionAlarm Severity: Minor/Major Log: OVLD304	Cause: This alarm is generated when an overload detection alarm is received from an MG 9000. Indicates a performance trouble has occurred. Action: Calls may be lost. Check the resource usage for this network element.
Type: ovldRscMonPduRateFault Severity: Warning Log: OVLD800	Cause: This alarm is generated when an Pdu rate overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: ovldRscMonCbvMsgRFault Severity: Warning Log: OVLD801	Cause: This alarm is generated when an Cbv message rate overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: ovldRscMonConnQueFault Severity: Warning Log: OVLD802	Cause: This alarm is generated when an connection queue overloaded alarm is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: ovldRscMonCpuUtilFault Severity: Warning Log: OVLD803	Cause: This alarm is generated when an CPU utilization fault is received from an MG 9000. Indicates a threshold has been crossed. Action: None, for information only.
Type: perfMonCpuFault Severity: Warning Log: OVLD804	Cause: This alarm is generated when a CPU utilization overloaded alarm is received from an MG 9000. Action: None, for information only.
Type: perfMonRamFault Severity: Warning Log: OVLD805	Cause: This alarm is generated when a PM RAM utilization fault is received from an MG 9000. Action: None, for information only.
Type: perfMonFlashFault Severity: Warning Log: OVLD806	Cause: This alarm is generated when a PM flash utilization fault is received from an MG 9000. Action: None, for information only.

DS-512 card alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: perfMonChannFault Severity: Warning Log: OVLD807	Cause: This alarm is generated when a PM channel utilization fault is received from an MG 9000. Action: None, for information only.
Type: PatchAlarmFault Severity: Major Log: PATC301	Cause: This alarm is generated when a patch alarm fault is received on an MG 9000 DS-512 card indicating a restart is required after a patch has been removed or applied. Action: Restart the affected card by performing the procedure Restarting a card on page 348.

Clearing MG 9000 CES alarms

Purpose of this procedure

This section identifies the CES alarms generated for the DS1 card, the alarm severity, the log report, the cause of the alarm, and the recovery methods. CES alarms are derived from faults detected by the DS1 cards or from faults with the DS1 card. Carrier maintenance also reports these DS1 alarms to the MG 9000 Manager. CES only reports faults for carriers on which services are running.

When to use this procedure

Use this procedure when MG 9000 CES alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a CES fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

CES alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Loss of cells Severity: None Log: CES305	Cause: No cells are being received from the ATM network. Action: Make sure the OC-3 card is unlocked. Check ATM virtual circuit is connected. Check the status of far side equipment. The alarm will be cleared when the ATM connection is restored.

Clearing MG 9000 carrier alarms

Purpose of this procedure

This procedure identifies the carrier alarms generated for the DS1 and OC-3/STM-1 carriers, the alarm severity, the log report, the cause of the alarm, and the recovery methods. Carrier alarms are derived from faults detected by the DS1 and DCC cards. Carrier maintenance reports the following alarms to the MG 9000 Manager.

> ***Note:*** Terminal/inward loopbacks can be useful in determining if an alarm is the result of problems with local equipment, or the far-end equipment or the fiber/cable. When this type of loopback is applied and the alarm clears, the problem is typically at the far end or with the cable/fiber connector. Loopbacks can only be used on locked carriers. Typically, after initial commissioning, carriers can be locked only on the inactive card.

When to use this procedure

Use this procedure when MG 9000 carrier alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a carrier fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Loss of signal (LOS) Severity: DS1 - Minor, OC3 - Critical Log: MGCA301	Cause: Loss of signal for DS1 or OC-3 Action: OC-3 - Check the Rx fiber cable on the DCC-OC3 card. Make sure the cable is connected and that the Rx and Tx fiber connectors are not swapped at the card’s fiber receptacle. Check the fiber cable and connectors and replaced if damaged. Check that the fiber is routed and connected to the far-end equipment and the far-end has enabled/unlocked the carriers. DS1 - Make sure the cable connector is properly attached. Check far-end cable for the problem is likely at the far end.
Type: Alarm indication signal (AIS) Severity: DS1 - Minor, OC3 - critical Log: MGCA302	Cause: Alarm indication signal for DS1 or OC-3 Action: OC-3 or DS1 - If LOS or LOF is also present, then troubleshoot LOS or LOF alarm types. Otherwise check far end equipment for carrier alarms. Also, check far-end equipment for carrier locked or disabled. Often, if far-end equipment is locked, it will transmit AIS alarm.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: Loss of frame (LOF) Severity: DS1 - Minor, OC3 - critical Log: MGCA303	Cause: Loss of frame Action: OC-3 - If LOS alarm is also present, troubleshoot LOS alarm. Check the Rx fiber cable on the DCC-OC3 card. Make sure the cable is properly connected and that the Rx and Tx fiber connectors are not swapped at the card's fiber receptacle. Check the fiber cable and connectors for damaged. If the fiber cable is damaged, replace it. Check clock sync or timing problems. DS1 - Make sure the cable connector is properly attached. Check far-end cable, indicating the problem is likely at the far end. Check clock sync or timing problems.
Type: bit error ratio signal fail (BERSF) Severity: Critical Log: MGCA305	Cause: Bit error rate signal failure on OC-3 Action: Check far-end equipment for alarms. Check fiber/connectors. If alarm does not clear, check clock sync or check for far-end timing problems.
Type: bit error ratio signal degrade (BERSD) Severity: Major Log: MGCA306	Cause Bit error rate signal degrade on OC-3 Action: Check far-end equipment for alarms. Check fiber/connectors. If alarm does not clear, check clock sync or check for far-end timing problems.
Type: remote defect indication (RDI) Severity: Minor Log: MGCA307	Cause: Remote defect indication on OC-3 Action: Check the carrier and make sure it is unlocked. Check far-end equipment for alarms. An RDI-L (line) typically indicates the local carriers have not been unlocked (meaning the laser is off). If an RDI-P (path) persists, check far-end equipment for alarms.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: path label mismatch (PLM) Severity: Minor Log: MGCA308	Cause: Path label mismatch on OC-3 Action: Path label appears to be set incorrectly at far end. Check far-end equipment for proper provisioning. Path Label should be set for ATM (0x13). Check for other local carrier alarms. If problem persists, replace the DCC card. Go to Replacing a DCC card. If problem persists, restart DCC card.
Type: loss of pointer (LOP) Severity: Minor Log: MGCA309	Cause: Loss of pointer on OC-3 Action: If other local carrier alarms exist, take action to correct those alarms first. Check far-end equipment for correct provisioning. Check far-end equipment for alarms. Check fiber/connectors. Check fiber/connectors. If alarm does not clear, check clock sync or check for far-end timing problems. If problem persists, restart DCC card. If problem persists, replace the DCC card. Go to Replacing a DCC card.
Type: Uneq Severity: Minor Log: MGCA310	Cause: Unequipped on OC-3 Action: If other local carrier alarms exist, take action to correct those alarms first. Check far-end equipment for correct provisioning. Check far-end for carrier alarms. Check fiber/connectors. If alarm does not clear, check clock sync or check for far-end timing problems. If problem persists, restart DCC card. If problem persists, replace the DCC card. Go to Replacing a DCC card.
Type: imaLinkLif Severity: Major Log: MGCA312 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA Link - Loss of IMA frame Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: imaLinkLods Severity: Major Log: MGCA313 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA Link - Loss of delayed synchronization Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.
Type: imaLinkRfi Severity: Major Log: MGCA314 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA Link - Remote failure indication Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.
Type: imaLinkTxMisConnect Severity: Major Log: MGCA315 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA Link transmit misconnect Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: imaLinkRxMisConnect Severity: Major Log: MGCA316 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA Link receive misconnect Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.
Type: imaLinkTxFault Severity: Major Log: MGCA317 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA Link transmit fault Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.
Type: imaLinkRxFault Severity: Major Log: MGCA318 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA link receive fault Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.
Type: imaLinkTxUnusableFe Severity: Minor Log: MGCA319 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA link transmit unusable far end Action: Look at why the Multiservice Switch says it is unusable. Check the physical layer on the Multiservice Switch and determine if there is an alarm or performance measurement errors there first. If not, check the transmit and receive stuff performance measurements on the Multiservice Switch. The transmit and receive stuff values should be incrementing.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: imaLinkRxUnusableFe Severity: Minor Log: MGCA320 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA link receive unusable far end Action: Look at why Multiservice Switch says it is unusable. Check the physical layer on the Multiservice Switch and determine if there is an alarm or performance measurement errors there first. If not, check the transmit and receive stuff performance measurements on the Multiservice Switch. The transmit and receive stuff values should be incrementing.
Type: imaGroupStartupFe Severity: Major Log: MGCA321 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA group startup far end Action: Check that the MG 9000 and Multiservice Switch configuration parameters match. Examples of the configuration parameters are: IMA version, group ids, clocking, framer length, symmetry, min transmit/receive links.
Type: imaGroupCfgAbort Severity: Critical Log: MGCA322 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA group configuration abort Action: Check that the MG 9000 and Multiservice Switch configuration parameters match. Examples of the configuration parameters are: IMA version, group ids, clocking, framer length, symmetry, min transmit/receive links.
Type: imaGroupCfgAbortFe Severity: Major Log: MGCA323 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA group configuration abort far end Action: Check that the MG 9000 and Multiservice Switch configuration parameters match. Examples of the configuration parameters are: IMA version, group ids, clocking, framer length, symmetry, min transmit/receive links.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: imaGroupInsuffLinks Severity: Critical Log: MGCA324 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA group insufficient links Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.
Type: imaGroupInsuffLinksFe Severity: Major Log: MGCA325 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA group insufficient links far end Action: Determine why the links are down. Check the physical layer on the MG 9000 to see if there is an alarm or performance errors. If not, check the transmit and receive stuff performance measurements at the IMA level for the link. The transmit and receive stuff values should be nearly equal. If not, there must be a physical reason why the ICP cells are not being passed properly.
Type: imaGroupBlockedFe Severity: Minor Log: MGCA326 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA group blocked far end Action: Determine that the group on Multiservice Switch is unlocked.
Type: imaGroupTimingSynch Severity: Major Log: MGCA327 ***Note:*** Only applies if a DS1-IMA card is provisioned.	Cause: IMA group timing synchronization Action: Check that the group on the Multiservice Switch is CTC.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: abiLossofClock Severity: Critical Log: MGCA328 ***Note:*** Only applies if a DS-512 card is provisioned.	Cause: ABI loss of clock on DS-512 optical link Action: Verify the fibers are in good condition. Check the fibers with a light meter. If the fibers are bad, replace the fiber cables. If the fibers are in good condition, clean the fibers. Verify the fiber connections between the ABI and XPM are correct.
Type: abiLossofFrame Severity: Critical Log: MGCA329 ***Note:*** Only applies if a DS-512 card is provisioned.	Cause: ABI loss of frame on DS-512 optical link Action: Verify the fibers are in good condition. Check the fibers with a light meter. If the fibers are bad, replace the fiber cables. If the fibers are in good condition, clean the fibers. Verify the fiber connections between the ABI and XPM are correct
Type: abilowlightlevel Severity: Critical Log: MGCA330 ***Note:*** Only applies if a DS-512 card is provisioned.	Cause: ABI loss of signal (low light level) on DS-512 optical link Action: Verify the fibers are in good condition. Check the fibers with a light meter. If the fibers are bad, replace the fiber cables. If the fibers are in good condition, clean the fibers. Verify the fiber connections between the ABI and XPM are correct
Type: abiChannelParityError Severity: Minor Log: MGCA331 ***Note:*** Only applies if a DS-512 card is provisioned.	Cause: ABI channel parity error on DS-512 optical link Action: Verify the fibers are in good condition. Check the fibers with a light meter. If the fibers are bad, replace the fiber cables. If the fibers are in good condition, clean the fibers. Verify the fiber connections between the ABI and XPM are correct
Type: Trace identifier mismatch Severity: Minor Log: MGCA332 ***Note:*** Applies to SDH only.	Cause: Trace identifier mismatch (TIM) alarm for the received path trace identifier is generated when the received path trace identifier does not match what is provisioned at the MG 9000. Action: Perform the Capturing current path trace identifier value on an STM-1 port in this section.

Carrier alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: AlarmIndicationSignal Severity: Major Log: MGCA333	Cause: A DS3 alarm indication signal was received on DS3. Action: If DS3 LOF alarm is also present, then troubleshoot the LOF alarm. Otherwise, check the far end for a locked carrier or disabled equipment.
Type: DS3LossOfFrame Severity: Major Log: MGCA334	Cause: A loss of frame was received on DS3. Action: Troubleshoot OC3 alarm first, if present. Check far end DS3 connectors. Check clock sync or timing problems.
Type: DS3RemoteAlarmIndicationSignal Severity: Minor Log: MGCA335	Cause: A remote alarm indication was received on DS3. Action: Check the carrier and ensure it is unlocked. Check far end equipment for DS3 alarms.

The following procedure is a user-initiated action to return the active carrier to the active card. These conditions are depicted as configuration numbers 1 and 3 shown in the “Protection switch graphical representations” table.

> ***Note:*** When a mode mismatch occurs with the far end, and the APS Maintenance or APS Provisioning GUI is open, a message appears warning of this condition. On the Shelf View, an X icon appears with the other APS carrier state icons. When the mismatch is corrected, the X icon on the Shelf View and Card View will clear.

Recovery from APS split-mode

At your current location

1 Clear the fault that caused the alarm using the actions provided in the Carrier alarms table.

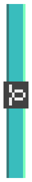
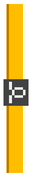
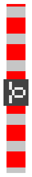
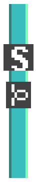
At the MG 9000 Manager

2 At the Subnet View, double click on the MG 9000 node icon on which the APS split -mode recovery must be performed. The Frame View appears.

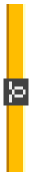
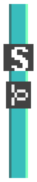
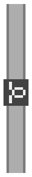
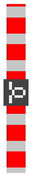
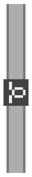
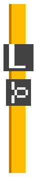
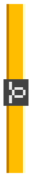
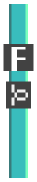
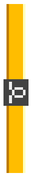
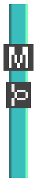
3. At the Frame View, double click on the master shelf. The Shelf View appears.
4. At the Shelf View double, click on the Active OC-3 card. The OC-3 Card View appears.
5. At the OC-3 Card View, double click on the OC-3 port (STM-1 port). The OC-3 Port View (or STM-1 Port View) appears.
6. At the OC-3 Port View (STM-1 Port View), launch the APS Maintenance View.
7. Using the Protection Switch Commands pull-down, select and apply command: ManualSwitch Protected to Working Carrier.
8. Verify that the graphical protection switch indicators that are visible at the Shelf or Card View returned to condition Number 1 as shown in the “Protection switch graphical representations” table.
9. This procedure is complete.

The following table identifies the graphical representations of carrier states seen at the master shelf view and DCC card views.

Protection switch graphical conditions

Number	Active	Standby	Condition description
1			Working to Normal and Protected Line Ready to Spare This is the expected normal configuration.
2			Working Line Troubled and Protected line Switched and unprotected (APS). (The carrier is troubled when either the card or the carrier has alarms on it, the card’s or carrier’s Operational status is not “Up”, or the card’s or the carrier’s Administrative state is “Locked”)

Protection switch graphical conditions

Number	Active	Standby	Condition description
3			Working Line returned to normal after APS and is ready to revert. Protected line is Switched.
4			Working Line Unprotected, Protected Line Troubled or carrier is unlocked.
5			Working Line Unprotected, Protected Line No Trouble but locked out
6			Working Line returned to normal after APS and ready to revert. Protected Line is switched.
7			Working Line ready to revert and Protection Line is Forced/Manual Switched.

Use the following procedure to capture the current path trace identifier to clear a trace identifier mismatch alarm on an STM-1 port.

Capturing current path trace identifier value on an STM-1 port

At the MG 9000 Manager

1 From the Frame View, double click on the master shelf. The Shelf View appears.

2 From the Shelf View, double click on the DCC card. The OC-3 Card View appears.

3 From the OC-3 Card View, double click on the STM-1 Port. The STM-1 Port View appears.

4 Click on Rx Trace Capture in the Path pane of the STM-1 Port View. This instructs the MG 9000 to capture and use the currently received Path Trace Identifier as being correct, and the alarm will clear.

5 This procedure is complete.

Maintaining OC-3 automatic protection switching

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 node icon. The Frame View appears.

2 At the Frame View, double click on the master shelf. The Shelf View appears.

3 At the Shelf View, if there are two OC-3 cards in the master shelf, double click on the Active OC-3 card. The OC-3 Card View appears.

4 At the OC-3 Card View, double click on the OC-3 port. The OC-3 Port View appears.

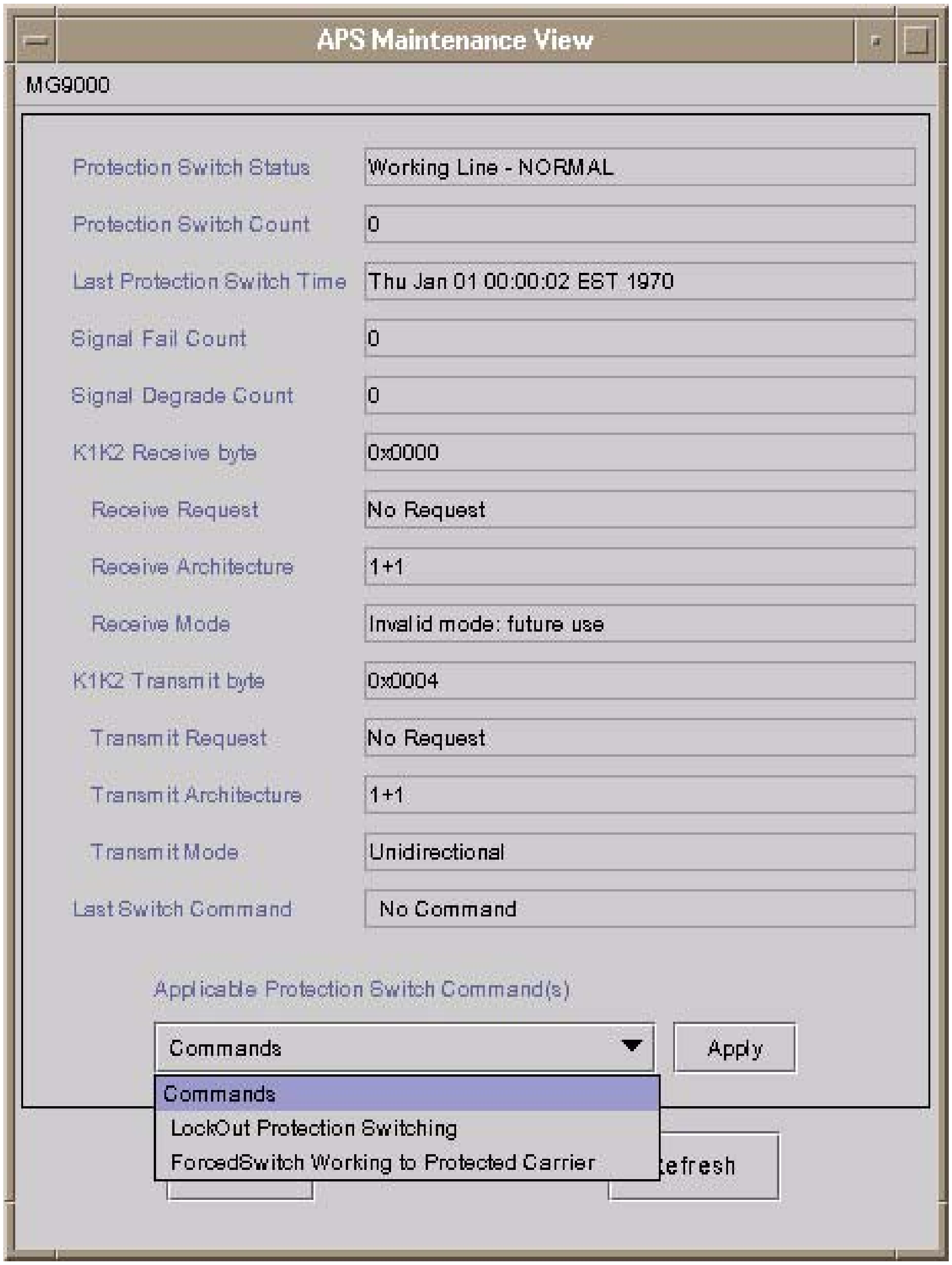
5 At the OC-3 Port View, launch the APS Maintenance View.

The APS Maintenance View shows the

- Protection Switch Status
- Protection Switch Count
- Last Protection Switch Time
- Signal Fail Count
- Signal Degrade Count
- Transmit and receive data
- Last Switch Command

The Protection Switch Commands may only be exercised from the APS Maintenance View launched from the OC-3 port on the active OC-3 card. The APS Maintenance View is shown next.

APS Maintenance View with protection switch commands shown



APS Maintenance View

MG9000

Protection Switch Status	Working Line - NORMAL
Protection Switch Count	0
Last Protection Switch Time	Thu Jan 01 00:00:02 EST 1970
Signal Fail Count	0
Signal Degrade Count	0
K1K2 Receive byte	0x0000
Receive Request	No Request
Receive Architecture	1+1
Receive Mode	Invalid mode: future use
K1K2 Transmit byte	0x0004
Transmit Request	No Request
Transmit Architecture	1+1
Transmit Mode	Unidirectional
Last Switch Command	No Command

Applicable Protection Switch Command(s)
Commands
Apply
Commands
LockOut Protection Switching
ForcedSwitch Working to Protected Carrier
Refresh

6 Set the OC-3 to the desired state using the Commands pull-down and select Apply.

> ***Note:*** The list of commands displayed varies according to the state of the carrier. The Commands pull-down is only accessible on the active card.

The following table lists the commands and their effect on the carrier. The commands visible at the command pull-down depends on the condition of the carriers.

Applicable Protection switch commands

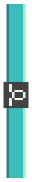
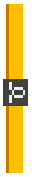
Command	Effect
LockOut Protection Switching	Disables Automatic Protection Switching and manual/Force Protection Switching features by locking out the protected (spare) carrier. ***Note:*** During a lockout of protection switching, call processing redundancy will be at risk since the APS feature is disabled/locked Out.
ForcedSwitch Working to Protected Carrier	Forces a manual protection switch from working (normal) carrier to protected (spare) carrier by overriding minor failure conditions. This command, in effect, forces the Active controller card to use the fiber on the INactive card. If failure conditions are major or excessive on the protected carrier, this command will be rejected.
ManualSwitch Working to Protected Carrier	Manual protection switch from working (normal) carrier to protected (spare) carrier. This command, in effect, allows the Active controller card to use the fiber on the INactive card. This may be useful when repairing a fiber on the ACtive card. This command will be rejected if signal fail conditions exist on the protected carrier or the Inactive carrier of the card is locked.

Applicable Protection switch commands

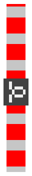
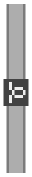
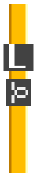
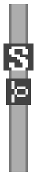
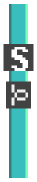
Command	Effect
ForcedSwitch Protected to Working Carrier	Forces a manual protection switch from protected (spare) carrier to working (normal) carrier by overriding minor failure conditions. This, in effect, forces the Active controller to use its own fiber. ***Note:*** This command is only available when the carriers are currently switched (for example, APS mode). If failure conditions are excessive on the working carrier, this command will be rejected.
ManualSwitch Protected to Working Carrier	Manual Protection switch from protected (spare) carrier to working (normal) carrier. This, in effect, allows the Active controller card to use its own fiber. Typically, this command is recommended to switch BACK to the working (normal) carrier after a carrier defect has been cleared.

The icons visible on the shelf/card view identify the carrier states. The different states are listed in the following table.

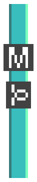
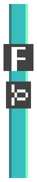
APS Shelf/Card View Icons and meaning

Icon	Meaning
	The OC3 Carrier is in an untroubled state. The OC3 Card and Carrier Admin State is Unlocked and Operational state is Up/Enabled. This is the normal configuration for the Active OC-3 carrier.
	The OC3 Carrier is untroubled and ready to handle the protection switch (APS). This is the normal configuration for the Standby OC-3 carrier.

APS Shelf/Card View Icons and meaning

Icon	Meaning
	The carrier is troubled, that is, either the card or the carrier has alarms on it, the card’s or carrier’s Operational status is not “Up”, or the card’s or the carrier’s Administrative state is “Locked”.
	The carrier is untroubled but not protected. Its mate carrier is troubled or locked out and is not ready for protection switch.
	The carrier is locked out for protection switching
	The carrier is switched and unprotected.
	The carrier is switched and protected. The mate carrier is ready to switch back.

APS Shelf/Card View Icons and meaning

Icon	Meaning
	The carrier is manually switched
	The carrier is forced switched.

7 This procedure is complete.

Clearing MG 9000 xDSL alarms

Purpose of this procedure

This procedure identifies the alarms generated for the xDSL card, the alarm severity, the log report, the cause of the alarm, and the recovery methods. xDSL alarms are derived from faults detected by the xDSL cards or from faults with the xDSL card.

When to use this procedure

Use this procedure when MG 9000 xDSL card alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a xDSL fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

xDSL alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: noClock Severity: Critical Log: xDSL310	Cause: No clock (local modem clock failure) Action: If this is a persistent problem, change the provisioning values for the circuit to improve immunity to loop impairments or replace the remote modem or line card.
Type: handshakeFail Severity: Critical Log: xDSL311	Cause: Hand shake failed (protocol error) Action: If this is a persistent problem, change the provisioning values for the circuit to improve immunity to loop impairments or replace the remote modem or line card.

xDSL alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: linkMismatch Severity: Critical log: xDSL312	Cause: Link mismatched (configuration error) Action: If this is a persistent problem, change the provisioning values for the circuit to improve immunity to loop impairments or replace the remote modem or line card.
Type: vpiNonzero Severity: Critical Log: xDSL313	Cause: VPI is not zero. ATM traffic dropped at WAC - upstream Action: If persistent, reset and/or reseat the line card. If this does not clear the alarm, replace the line card.
Type: lcdIATUC Severity: Critical Log: xDSL314	Cause: ATUC line code initialization failure (loss of sync of ATM cells - upstream) Action: If persistent, reset and/or reseat the line card. If this does not clear the alarm, replace the line card.
Type: lcdIATUR Severity: Critical Log: xDSL315	Cause: ATUR line code initialization failure (loss of sync of ATM cells - downstream) Action: If persistent, reset and/or reseat the line card. If this does not clear the alarm, replace the line card.
Type: failATUC Severity: Critical Log: xDSL316	Cause: Fail in ATUC remote line (local modem critical - not responding, in Kernal mode, download failure or message corrupted) Action: If persistent, reset and/or reseat the line card. If this does not clear the alarm, replace the line card.
Type: circuitHardwareFault Severity: Critical Log: xDSL317	Cause: Circuit hardware fault Action: Replace the line card.
Type: losATUC Severity: Minor Log: xDSL301	Cause: Loss of signal in local modem Action: Generally, this indicates the customer premise equipment (CPE) has been powered off. If subscriber complains, it may indicate loop impairment or faulty modem. Check subscriber connection to modem.

xDSL alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: lofATUC Severity: Minor Log: xDSL302	Cause: Loss of frame in local modem Action: Generally, this indicates the customer premise equipment (CPE) has been powered off. If subscriber complains, it may indicate loop impairment or faulty modem. Check subscriber connection to modem.
Type: lprATUC Severity: Minor Log: xDSL303	Cause: Loss of power in ATUC line Action: Reset and/or reseat line card. Check the power supply to the shelf and line card.
Type: lolATUC Severity: Minor Log: xDSL304	Cause: Loss of link in ATUC line Action: Generally, this indicates the customer premise equipment (CPE) has been powered off. If subscriber complains, it may indicate loop impairment or faulty modem. Check subscriber connection to modem.
Type: losATUR Severity: Minor Log: xDSL305	Cause: Loss of signal in ATUR remote end line Action: Generally, this indicates the customer premise equipment (CPE) has been powered off. If subscriber complains, it may indicate loop impairment or faulty modem. Check subscriber connection to modem.
Type: lofATUR Severity: Minor Log: xDSL306	Cause: Loss of frame in ATUR remote end line Action: Generally, this indicates the customer premise equipment (CPE) has been powered off. If subscriber complains, it may indicate loop impairment or faulty modem. Check subscriber connection to modem.
Type: lprATUR Severity: Minor Log: xDSL307	Cause: Loss of power in ATUR remote end line Action: None. This alarm signifies a normal power off condition from the remote modem.

xDSL alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: lolATUR Severity: Minor Log: xDSL308	Cause: Loss of link in ATUR remote end line Action: Generally, this indicates the customer premise equipment (CPE) has been powered off. If subscriber complains, it may indicate loop impairment or faulty modem. Check subscriber connection to modem.
Type: aturNotPresent Severity: Minor Log: xDSL309	Cause: ATUR remote line is not present Action: If this is a persistent problem, change the provisioning values for the circuit to improve immunity to loop impairments or replace the remote modem or line card.
Type: adslAturRateChangeTrap Severity: None Log: xDSL602	Cause: The ATURs transmit rate has changed (RADSL mode only). Action: None, for information only.
Type: adslAtucPerfLofsThreshTrap Severity: None Log: xDSL800	Cause: Loss of Framing in a 15-minute interval threshold reached. Action: None, for information only.
Type: adslAtucPerfLossThreshTrap Severity: None Log: xDSL801	Cause: Loss of Signal in a 15-minute interval threshold reached. Action: None, for information only.
Type: adslAtucPerfLprsThreshTrap Severity: None Log: xDSL802	Cause: Loss of Power in a 15-minute interval threshold reached. Action: None, for information only.
Type: adslAtucPerfESsThreshTrap Severity: None Log: xDSL803	Cause: Errored second in a 15-minute interval threshold reached. Action: None, for information only.
Type: adslAturPerfLofsThreshTrap Severity: None Log: xDSL804	Cause: Loss of link in a 15-minute interval threshold reached. Action: None, for information only.

xDSL alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: adslAturPerfLofsThreshTrap Severity: None Log: xDSL805	Cause: Loss of Framing in a 15-minute interval threshold reached. Action: None, for information only.
Type: adslAturPerfLossThreshTrap Severity: None Log: xDSL806	Cause: Loss of Signal in a 15-minute interval threshold reached. Action: None, for information only.
Type: adslAturPerfLprsThreshTrap Severity: None Log: xDSL807	Cause: Loss of Power in a 15-minute interval threshold reached. Action: None, for information only.
Type: adslAturPerfESsThreshTrap Severity: None Log: xDSL808	Cause: Errored second in a 15-minute interval threshold reached. Action: None, for information only.
Type: nnDSLThresholdTrap Severity: None Log: xDSL809	Cause: Indicates a DSL interface has exceeded the specified threshold on a given performance measurement, specified by the following nnDSLThresholdNotifyType: • atucfec (1) • atuccrc (2) • atucncd (3) • atucocd (4) • atuchec (5) • atuclcd (6) • aturfec (7) • aturblockError (8) • aturncd (9) • aturocd (10) • aturhec (11) • aturlcd (12) Action: None, for information only.

Clearing MG 9000 ATM alarms

Purpose of this procedure

This procedure identifies the ATM alarms generated for the DCC card, the alarm severity, the log report, the cause of the alarm, and the recovery methods. ATM alarms are derived from faults detected by the DCC cards. The DCC card reports these alarms to the MG 9000 Manager.

When to use this procedure

Use this procedure when MG 9000 ATM alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with an ATM fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

ATM alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: vclTpAis Severity: Minor Log: VC301	Cause: ATM Vcl alarm indication signal Action: For xDSL, determine network element that has PVC cross-connect failure. Not applicable for private lines services.
Type: vclTpRdi Severity: Minor Log: VC302	Cause: ATM Vcl remote detection indicator Action: For PLoA services, take down the SVC and reestablish. For xDSL, determine network element that has PVC cross-connect failure.

ATM alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: vclLoc Severity: Minor Log: VC303	Cause: Loss of continuity, Vcl Action: Disable continuity check on this circuit. For PLoA services, take down the SVC and reestablish circuit. For xDSL, determine network element that has PVC cross-connection failure.
Type: vccTpAis Severity: Minor Log: VC304	Cause: ATM Vcc alarm indication signal Action: For PLoA services, isolate DS1 carrier at the far end connection. For xDSL, determine network element that has PVC cross-connect failure.
Type: vccTpRdi Severity: Minor Log: VC305	Cause: ATM Vcc remote detection indicator Action: For PLoA services, take down the SVC on this circuit and reestablish the circuit. For xDSL, determine network element that has PVC cross-connect failure.
Type: vccLoc Severity: Minor Log: VC306	Cause: Loss of continuity, Vcc Action: Disable continuity check on this circuit. For PLoA services, take down the SVC and reestablish the circuit. For xDSL, determine network element that has PVC cross-connect failure.

ATM alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: UNI connection failure Severity: Minor Log: XPKT301, seen at the Core	Cause: Generated at the Core when a UNI release/release complete message is received by an MG 9000 or an MG 9000 ABI peripheral where the release cause in the message indicates an ATM switched virtual connection (SVC) call setup failure. Action: None, for information only. Use this report to diagnose call completion problems.
Type: UNI Mid-call failure Severity: Minor Log: XPKT302, seen at the Core	Cause: Generated at the Core when a UNI release/release complete message is received by an MG 9000 or MG 9000 ABI peripheral where the release cause in the message indicates a failure, that is, not normal clearing, for established calls. Action: None, for information only. Use this report to diagnose call completion problems.

Clearing bandwidth manager alarms and notifications

Purpose of this procedure

This procedure lists the bandwidth manager alarms. Bandwidth manager alarms are minor alarms and are viewed at the MG 9000 Manager Alarm Browser. The alarm types called notifications are sent to the MG 9000 Manager log when they are received.

When to use this procedure

Use this procedure when MG 9000 bandwidth manager alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a bandwidth fault in the Alarm Browser by using the following steps.

1. Select an alarm in the Alarm Browser
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

nnBwFault Bandwidth alarms

Alarm type, severity, associated alarm message, and log report	Cause, duration, association, and action
Type: bwResBandwTotalFault Severity: warning Alarm message: “Network Interface Overall Reserved Bandwidth Alarm” Log: BW301	Cause: Reserved bandwidth use on the network interface has exceeded the Bandwidth Congestion Threshold. Duration: Clears when the reserved bandwidth falls 10% below the threshold value crossed. Association: History data for total network interface reserved bandwidth. Action: Monitor network interface bandwidth usage. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the network interface bandwidth usage.

nnBwFault Bandwidth alarms

Alarm type, severity, associated alarm message, and log report	Cause, duration, association, and action
Type: bwSwitchFabricTotalFault Severity: warning Alarm message: “Overall Cell Queue Congestion Alarm” Log: BW304	Cause: Overall ATM cell queue is at least 90% full. Duration: Clears when the overall cell queue fill is less than 80% full. Association: History data for overall cell queue fill levels. Action: Monitor the overall queue fill level fullness. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the overall fill level fullness.
Type: bwResBandwSloaFault Severity: warning Alarm message: “Network Interface SLoA Reserved Bandwidth Alarm" Log: BW302	Cause: Reserved bandwidth dedicated to switched lines connections on the network interface has exceeded the Bandwidth Congestion Threshold with respect to the amount of bandwidth configured on the network interface for switched lines. Duration: Clears when switched lines reserved bandwidth on the network interface is 10% less than the threshold. Association: History data for switched lines reserved bandwidth. Action: Increase the configured reserved bandwidth for switched lines if desired. Monitor total network interface bandwidth use. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the total network interface bandwidth usage.

nnBwFault Bandwidth alarms

Alarm type, severity, associated alarm message, and log report	Cause, duration, association, and action
Type: bwSwitchFabricCbrFault Severity: warning Alarm message: “CBR Cell Queue Congestion Alarm” Log: BW305	Cause: ATM cell queue for this service type is at least 90% full. Duration: Clears when this service type cell queue is less than 80% full. Association: History data for overall cell queue fill levels and the CBR queue fill levels. Action: Monitor the overall queue fill level fullness. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the overall queue fill level fullness.
Type: bwSwitchFabricRtVbrFault Severity: warning Alarm message: “RT-BVRCell Queue Congestion Alarm” Log: BW306	Cause: ATM cell queue for this service type is at least 90% full. Duration: Clears when this service type cell queue is less than 80% full. Association: History data for overall cell queue fill levels and the RT-VBR queue fill levels. Action: Monitor the overall queue fill level fullness. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the overall queue fill level fullness.
Type: bwSwitchFabricNrtVbrFault Severity: warning Alarm message: “NRT-VBR Cell Queue Congestion Alarm” Log: BW307	Cause: ATM cell queue for this service type is at least 90% full. Duration: Clears when this service type cell queue is less than 80% full. Association: History data for overall cell queue fill levels and the NRT-VBR queue fill levels. Action: Monitor the overall queue fill level fullness. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the overall queue fill level fullness.

nnBwFault Bandwidth alarms

Alarm type, severity, associated alarm message, and log report	Cause, duration, association, and action
Type: bwSwitchFabricUbrFault Severity: warning Alarm message: "UBR Cell Queue Congestion Alarm" Log: BW308	Cause: ATM cell queue for this service type is at least 90% full. Duration: Clears when this service type cell queue is less than 80% full. Association: History data for overall cell queue fill levels and the UBR queue fill levels. Action: Monitor the overall queue fill level fullness. Go to "Using the Bandwidth Manager" in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the overall queue fill level fullness.
Type: bwSwitchFabricUbrPlusFault Severity: warning Alarm message: "UBR Cell Queue Congestion Alarm" Log: BW309	Cause: ATM cell queue for this service type is at least 90% full. Duration: Clears when this service type cell queue is less than 80% full. Association: Monitor the overall queue fill level fullness. Action: Monitor the overall queue fill level fullness. Go to "Using the Bandwidth Manager" in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the overall queue fill level fullness.

nnBwFault Bandwidth alarms

Alarm type, severity, associated alarm message, and log report	Cause, duration, association, and action
Type: bwSwitchFabricControlFault Severity: warning Alarm message: Control Channel Cell Queue Congestion Alarm” Log: BW310	Cause: ATM cell queue for this service type is at least 90% full. Duration: Clears when this service type cell queue is less than 80% full. Association: History data for overall cell queue fill levels and the CONTROL queue fill levels. Action: Monitor the overall queue fill level fullness. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the overall queue fill level fullness.
Type: bwResBandwAbiFault Severity: warning Alarm message: Log: BW311	Cause: Reserved bandwidth dedicated to ABI lines connections on the network interface has exceeded the bandwidth congestion threshold with respect to the amount of bandwidth configured on the network interface for switched lines. Duration: Clears when switched lines reserved bandwidth on the network interface is 10% less than the threshold. Association: History data for switched lines reserved bandwidth. Action: Increase the configured reserved bandwidth for switched lines if desired. Monitor total network interface bandwidth use. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on monitoring the total network interface bandwidth usage.

nnBwShelfBandwFault Bandwidth alarm information

Alarm type, severity, and associated alarm message	Cause, duration, association, and action
Type: bwResBandwShelfFault Severity: warning Alarm message: SLoA Shelf Reserved Bandwidth Alarm Log: BW300	Cause: Reserved bandwidth used on the indicated shelf has exceeded the Bandwidth Congestion Threshold. Duration: Clears when reserved bandwidth on the shelf is 10% below the Bandwidth Congestion Threshold. Association: Per shelf reserved bandwidth history tables can be checked to see if the current amount of reserved bandwidth on the shelf is out of the ordinary. Action: Increase threshold, try to decrease the number of active calls on the shelf, or take no action. Go to “Using the Bandwidth Manager” in *MG 9000 Configuration Management*, NN10096-511 for information on changing the threshold levels.

nnBwBandwUtilizationCongestion Bandwidth manager Notification events

Notification type	Description
totalInBandwUtil	Raised when the ingress utilization of the network interface exceeds the threshold set in nnBwReservedBandwCongestion. Notification can only be sent once every 15 minutes, so if ingress utilization is consistently exceeding the threshold a notification will be sent every 15 minutes. If one is not sent then the EM may assume the ingress utilization is not exceeding the threshold.
totalOutBandwUtil	Raised when the egress utilization of the network interface exceeds the threshold set in nnBwReservedBandwCongestion. Notification can only be sent once every 15 minutes, so if egress utilization is consistently exceeding the threshold a notification will be sent every 15 minutes. If one is not sent then the EM may assume the egress utilization is not exceeding the threshold.

nnBwSwitchFabricCongestion Bandwidth Manager Notification events

Notification type	Description
totalSwitchFab cbrSwitchFab rtVbrSwitchFab nrtVbrSwitchFab control ubrPlusSwitchFab ubrSwitchFab	Raised when the nnBwQueueCongestionThreshValue is exceeded by a particular cell queue. One condition is that the overall cell queue must be <75% full for the notification to be raised. These are 15 minute notifications and behave like the utilization notifications.

Clearing MG 9000 line alarms

Purpose of this procedure

This procedure identifies the line alarms generated, the alarm severity, the log report, the cause of the alarm, and the recovery methods. Line alarms are derived from faults detected by the DS1 cards. Carrier maintenance also reports these alarms to the MG 9000 Manager.

When to use this procedure

Use this procedure when MG 9000 line alarms are raised at the Alarm Browser.

Prerequisites

This procedure has no prerequisites.

Action

Correlate the faults listed in the following table with a line fault in the Alarm Browser by using the following steps:

1. Select an alarm in the Alarm Browser.
2. Look at the Description field of the Alarm Browser. The “Cause of alarm” column in the following table corresponds to the text that appears in the Description field.

> ***Note:*** If a fault affects a line circuit on a WLC, XDSL, GLC, or SAA card, the description field includes the Directory Number (DN) of the affected circuit. If no DN exists for the affected circuit, the description field reads "DN affected: None."

Line alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: lineFault Severity: MInor Log: SWLN301	Cause: Line fault Action: Perform line card diagnostic test and replace card if faulty.

Line alarms

Alarm type, severity, and log report	Cause of alarm and action
Type: lineProtectionFault Severity: Minor Log: SWLN302	Cause: Line protection fault Action: Remote source of high voltage. Perform line card diagnostic and replace card if faulty.
Type: lineBabbleState Severity: Minor Log: SWLN303	Cause: Line babble state Action: Perform line card diagnostic and replace card faulty.

Clearing MG 9000 audible alarms

The NTNY28 alarm relay card in the IBIP has six physical alarm relays that report critical, major and minor audible and visual alarms to the central office (CO) office alarm unit (OAU) or to other alarm reporting devices.

Critical, major and minor alarm events result in the corresponding audible and visual relays being set. When an alarm event is cleared, the DCC clears the audible and visual relays.

The audible and visual alarm relays are cleared (released) only when all alarms of the given severity have cleared.

The major audible and visual relay contacts are normally closed. When power to the NTNY28 alarm relay card in the IBIP is lost (power supply failure or the card is removed from the shelf), the major alarm relay contacts close immediately.

The alarm relay card in the IBIP supports an alarm cutoff feature (local and remote)

- local activation

  To activate the alarm cutoff, press and release the alarm cut-off (ACO)/lamp test switch on the front of the cooling unit in less than 2 seconds.

- remote activation

  A loop closure on the remote ACO leads found on the wire-wrap field on the IBIP alarm relay card activates the alarm cutoff feature.

The ACO feature silences the existing audible alarms, including dead system alarms driven by the audible alarm signals. The alarm cut-off capability does not inhibit (mask) subsequent CO audible/visual indications for additional or new alarms.

When combinations of the three alarm severity lamps are turned ON, they are initially put in a *wink* state, indicating a new alarm. When a technician presses the ACO switch, the applicable alarm changes from a *wink* state to a *steady* state. Unless the alarm clears, subsequent alarms resume the *wink* state for the applicable alarm.

The ACO generates a message to the MG 9000 Manager indicating an alarm acknowledgement. When the MG 9000 Manager acknowledges the alarm, the alarm state changes the indication from a *wink* state to a *steady* state. In this case, the steady state indicates the fault is being managed at the MG 9000 Manager.

Clearing MG 9000 Manager faults

Purpose of this procedure

This procedure identifies the faults that are generated for the MG 9000 Manager and the recovery methods.

The following table identifies the faults by component and the recovery responses in the MG 9000 Manager. The procedures that are referred to in the table appear in the Action section.

MG 9000 Manager faults and recovery responses

Component	Fault	Recovery response
GUI Client	Client displays an error dialog	Close error dialogs and retry operation If the problem persists, perform the Restarting a GUI client procedure for the GUI client. If the problem persists, perform the Restarting the mid-tier server procedure. If the problem persists, perform the Restarting the MG 9000 Manager procedure.
	GUI client process locks up or stops responding for extended period of time	Perform the Restarting a GUI client procedure for the GUI client If the problem persists, perform the Restarting the mid-tier server procedure If the problem persists, perform the Restarting the MG 9000 Manager procedure
	GUI client crashes while attempting an operation	Perform the Starting a GUI client procedure for the GUI client Retry the operation If the problem persists, perform the Restarting the mid-tier server procedure If the problem persists, perform the Restarting the MG 9000 Manager procedure

MG 9000 Manager faults and recovery responses

Component	Fault	Recovery response
GUI Client	GUI client displays the “blue screen of death” in Windows environment	Determine if an ATI Raedon 7000 series graphics card is installed on the desktop computer or an ATI Mobility graphics chip is installed in the laptop computer. Information on this issue be obtained from the Sun Bug Parade web site at http://developer.java.sun.com/developer/bugParade/bugs/4713003.html. Download the latest ATI Graphics drivers from the following web site or contact your IT support team for assistance: http://mirror.ati.com/support/driver.html.
	A communication failure occurs between the client and the mid-tier. The views will be forced closed. The following message appears: The communication to the mid-tier has been lost. This may be due to a network failure or the mid-tier may have been taken down. The client will be terminated. To continue working please launch the client again. If the problem persists after restarting the client please contact your administrator to verify the mid-tier is available for use. After clicking OK, the client will exit.	Perform the Starting a GUI client procedure for the GUI client Retry the operation If the problem persists, perform the Restarting the mid-tier server procedure If the problem persists, perform the Restarting the MG 9000 Manager procedure

MG 9000 Manager faults and recovery responses

Component	Fault	Recovery response
Mid-tier server	Mid-tier process stops responding (no log messages appearing in process log located at /var/adm/log/mg9kem/mg9kem.custlog)	Perform the Restarting the mid-tier server procedure If the problem persists, perform the Restarting the MG 9000 Manager procedure
Master servers: SAG (SNMP Access Gateway) EM Factory (MG 9000 Manager Factory) Subnet (Subnet Manager):	One or more of the afore-mentioned processes stop responding (no messages appearing in the corresponding logs located in /var/adm/log/mg9kem/mg9kem.custlog, see Naming conventions above)	Perform the Restarting the MG 9000 Manager procedure

The following procedures are used to clear MG 9000 Manager faults:

- Starting a GUI client
- Stopping a GUI client
- Restarting a GUI client
- Starting the mid-tier server
- Stopping the mid-tier server
- Restarting the mid-tier server
- Starting the master servers
- Stopping the master servers
- Restarting the master servers
- Starting the MG 9000 Manager
- Stopping the MG 9000 Manager
- Restarting the MG 9000 Manager
- Killing a UNIX process on the MG 9000 Manager

When to use this procedure

Use this procedure when clearing MG 9000 network element faults.

Prerequisites

The procedure has no prerequisites.

Action

The following table lists the alarms generated for the MG 9000 network element, the alarm severity, the log generated, and action to clear the alarm.

Network element alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: CommsLostToNE Severity: Critical Log: MGEM301	Cause: Generated when the MG 9000 Manager loses SNMP communication with the MG 9000. Action: Possible broken connection between the MG 9000 Manager and the MG 9000. Go to the Clearing MG 9000 network element alarm procedure that follows.
Type: AlarmsBeingThrottled Severity: Critical Log: MGEM303	Cause: Generated when the MG 9000 sends too many alarms within a 5 second window. Action: When this occurs, the MG 9000 Manager requests the MG 9000 stop sending alarms and this alarm is displayed. The condition clears when the number of alarms within a 5 second window falls below a set number.
Type: AlarmAuditFailed Severity: Critical Log; MGEM304	Cause: Alarm audit failure occurred. This indicates a communication failure between the MG 9000 Manager and the MG 9000. Action: Clear the communication problem. No other action is required. The alarm is cleared automatically when the next successful alarm audit occurs.

Network element alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: EncryptionKeyMismatch Severity: Critical Log; MGEM305	Cause: Either the network element (NE) encryption key or NE password being used on the MG 9000 Manager does not match the encryption key or password used on the MG 9000. Action: Verify that your passwords match. ***Note:*** if IPSec is enabled, the MGEM305 alarm will be raised by the MG 9000 Manager if the password on the MG 9000 Manager does not match the password on the MG 9000 Modify the encryption key at the NE properties view. The MGEM305 alarm can also be cleared by changing the key on the Local Craft Interface (LCI) and running an EM audit, or downloading a Public Key Infrastructure (PKI) certificate (if PKI digital signatures authentication is being used) For a detailed procedure, see Resolving an encryption key mismatch alarm.
Type: RequireAuditRecoveryExecuted Severity: Major Log: NE320	Cause: Generated when an audit recovery is executed. Action: None, for information only. However, if the alarm does not clear automatically, a manual audit or provisioning cleanup may be required.
Type: EmDbUnavailable Severity: Major Log: MGEM300	Cause: A VMG or termination provisioning action fails to write to the database. Action: No action required. When the database returns to service. The alarm clears when the next VMG or termination provisioning action successfully writes to the database.
Type: InvalidEMIPAddress Severity: Major Log: MGEM302	Cause: Communications subsystem failure; the MG 9000 Manager IP address provisioned on the MG 9000 is not valid. Action: Change the MG 9000 Manager IP address from the local craft interface (LCI)

Network element alarms

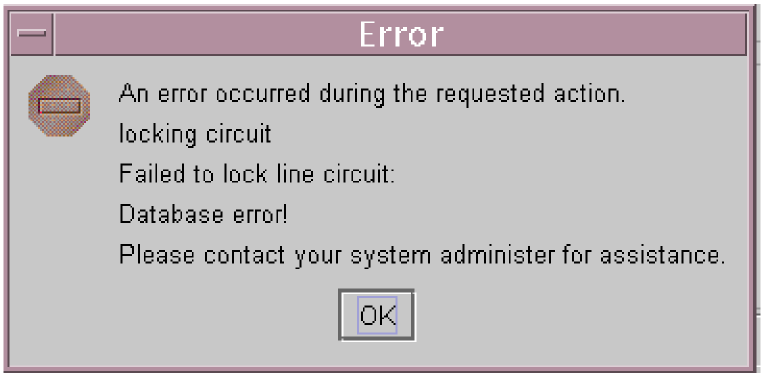
Alarm category, severity, and log report	Cause of alarm and action
Type: Databaseunavailable Severity: Warning Log: MGEM704	Cause: Database unavailable, correction failed. Action: None, for information only. The database will be corrected when it is available.
Type: Databasecorrected Severity: Warning Log: MGEM705	Cause: Database corrected. Action: None, for information only.
Type: SoftwareImageRequestedMG9K Severity: None Log: MGEM714	Cause: A user attempted to image an MG 9000 device. Action: None, for information only.
Type: SoftwareImageEvent Severity: None Log: NE609	Cause: Software image event. Action: None, for information only. If the Image status field indicates a failure, attempt to image the device again.
Type: AuditLogNotification Severity: None Log: MGAU600	Cause: Generated by the MG 9000 Manager when an Audit is started or stopped, a data mismatch was found between the MG 9000 and the MG 9000 Manager, or a communication failure occurred while the Audit was running. Action: None, for information only. For more information on the NE audit and the MGAU600 logs, refer to “Performing an MG9000 data audit” in *MG 9000 Configuration Management*, nn10096-511.

Network element alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: OMdatacollectionfailed Severity: Minor Log: OMC300	Cause: OM Collector failed to collect OM file from MG 9000 during collection event. Action: Check to see if the MG 9000 is traffic overloaded.
Type: OMdatacollectionfailedalarmcleared Severity: Minor Log: OMC300	Cause: OM Collector failed alarm cleared. Action: None, for information only.

Some data is persisted in the database. If a database error is encountered during MG 9000 Manager actions, an error is displayed to inform the user that the operation has failed due to a database error. Follow the instructions in the message. The following is an example of such an error message.

Error message



An error occurred during the requested action.

locking circuit

Failed to lock line circuit:

Database error!

Please contact your system administer for assistance.

Clearing MG 9000 network element alarm

At the MG 9000 Manager

1 Ping the IP address of the shelf DCC card to validate IP connectivity. Obtain the address from your network administrator.

2 Ping the IP address of the OAMP CIPOA port to validate IP connectivity. Obtain this address from your network administrator or by selecting Configuration->View/Modify NE Properties from the menu bar of the Subnet View and looking in the MG 9000 Manager IP Address field in the Properties View. This information call also be obtained from the CS 2000 SAM21 Manager, under the Shelf View, select IPoA Services and click on the Connections tab.

3 Check connectivity between the MG 9000 Manager and the MG 9000 using the Ping/Traceroute tool available from the Connection Test Tool. Access the Connection Test Tool using the Accessing the Connection test tool.

4 Check for status of the DCC card.

5 This procedure is complete.

Resolving an encryption key mismatch alarm

1 Ensure that the default NE password matches the password configured on the NE. For additional details on password administration, see *MG 9000 Security and Administration*, NN10162-611.

Note: The default password is the password you use to log in to the NE from the LCI.

2 Do one of the following steps:

If	Do
after verifying or resetting your passwords, the alarm persists	Step 3
after resetting your passwords, the alarm clears,	Step 4

3 Do one of the following steps, depending on the type of security authentication that is in use:

If	Do
If the Digital Control Card (DCC) on the NE is configured to use Digital Certificate Authentication	download the latest certificate. To download certificates, use procedure Downloading a valid certificate. See also *MG 9000 Security and Administration*, NN10162-611 and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
If the NE is configured to use Pre-shared Key (PSK) Authentication	Change the pre-shared key on the MG 9000 Manager and the MG 9000 NE. To do so, use procedure Changing the pre-shared key between the MG 9000 and the MG 9000 Manager. For details, see *MG 9000 Security and Administration*, NN10162-611 and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

4 This procedure is complete.

Downloading a valid certificate

Use the following procedure to download a valid certificate.

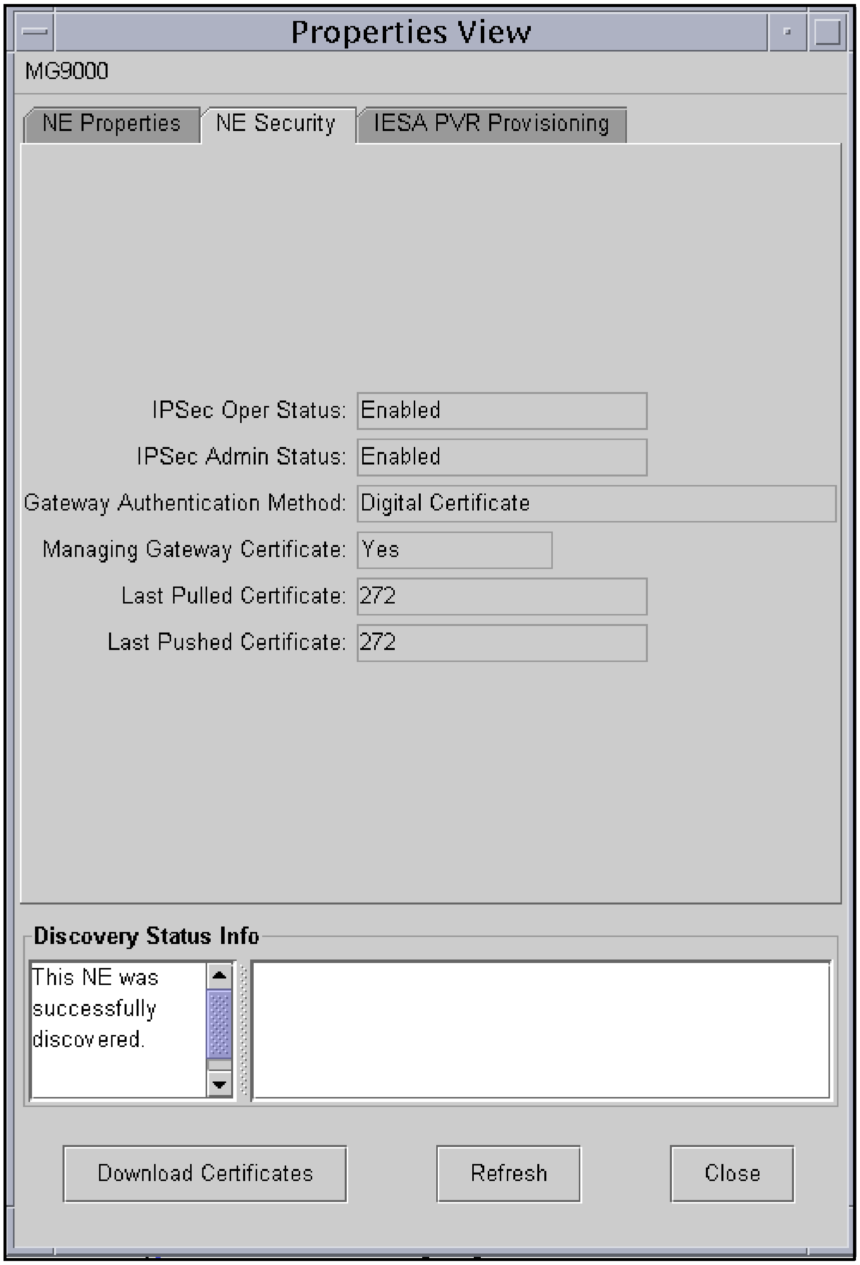
Downloading a valid certificate

At the MG 9000 Manager Subnet View

1 Choose a NE and select **Configuration > View/Modify NE Properties**. The Properties View appears.

2 Click the **NE Security** tab. The **NE Security** view appears:

Properties View showing the NE Security Properties View



IPSec Oper Status: Enabled

IPSec Admin Status: Enabled

Gateway Authentication Method: Digital Certificate

Managing Gateway Certificate: Yes

Last Pulled Certificate: 272

Last Pushed Certificate: 272

This NE was successfully discovered.

3 Click **Download Certificates** (this command requests and downloads a certificate to the MG 9000).

Watch the progress messages at the bottom of the GUI. The message indicates the success or failure of the MG 9000 EM to

- retrieve certificates from the IEMS
- download certificates to the MG 9000

4 You have completed this procedure.

Changing the pre-shared key between the MG 9000 and the MG 9000 Manager

Prerequisites

This procedure must only be performed in conjunction with the procedures documented in *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100.

> **CAUTION**
> **Risk of communication disruption, loss of service, or outage.**
> This procedure must only be performed in conjunction with the procedures documented in *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100.

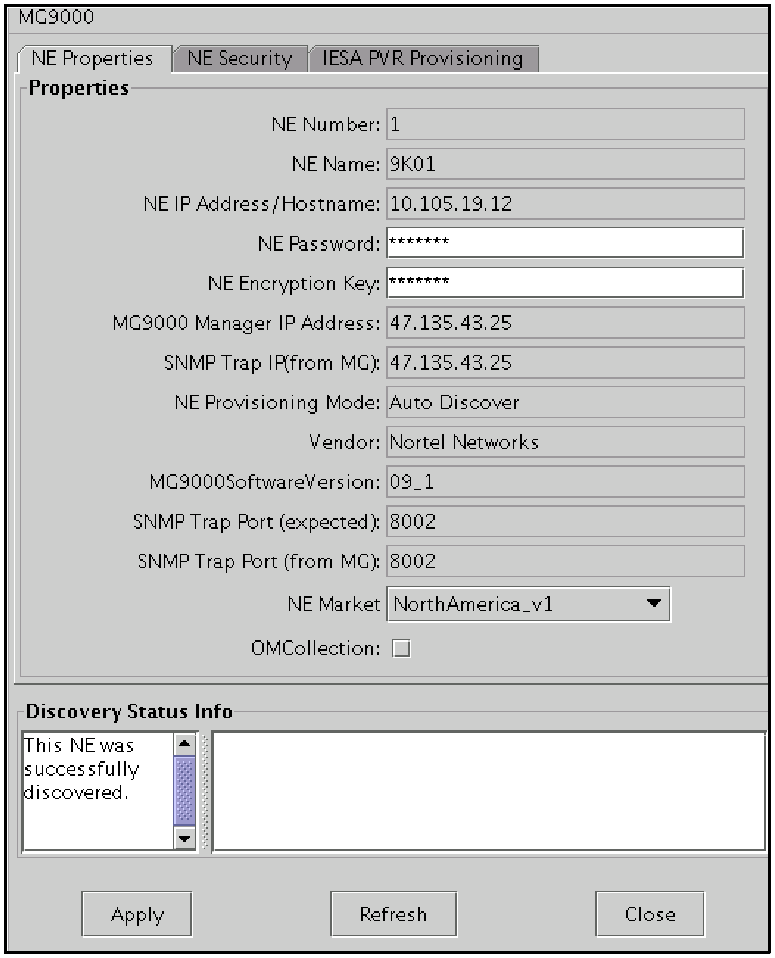
At the MG 9000 Manager

1 Launch the MG 9000 Manager web-based GUI hosted by the MG 9000 Manager midtier server.

2 From the MG 9000 Manager **Subnet View**, select **Configuration > View/Modify NE Properties > NE Properties**.

The NE Properties View appears:

MG 9000 NE Properties View



MG9000

Properties

NE Number: 1

NE Name: 9K01

NE IP Address/Hostname: 10.105.19.12

NE Password: *******

NE Encryption Key: *******

MG9000 Manager IP Address: 47.135.43.25

SNMP Trap IP(from MG): 47.135.43.25

NE Provisioning Mode: Auto Discover

Vendor: Nortel Networks

MG9000SoftwareVersion: 09_1

SNMP Trap Port (expected): 8002

SNMP Trap Port (from MG): 8002

NE Market NorthAmerica_v1

OMCollection: □

Discovery Status Info

This NE was successfully discovered.

3 Write down the IP address of the NE. You will require this information later in this procedure.

4 Modify the value in the NE Encryption Key field. Write down this value. You will require this information later in this procedure.

> ***Note:*** The encryption key must be 20 alphabetical characters (a-z, A-Z).

5 Click **Apply**.

At a PC or workstation with a web browser

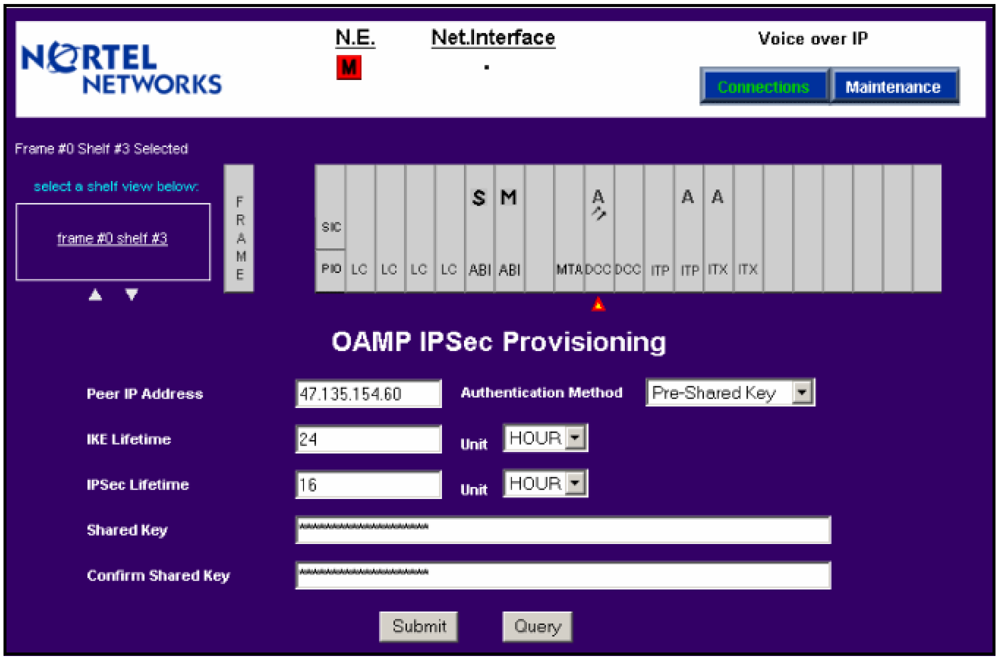
6 Go to the MG 9000 LCI GUI.

7 Select the active DCC card.

8 Click the active DCC and select the **IPSec Config > Provisioning** menu.

The OAMP IPSec Provisioning screen appears:

OAMP IPSec Provisioning screen



OAMP IPSec Provisioning

Peer IP Address: 47.135.154.60

Authentication Method: Pre-Shared Key

IKE Lifetime: 24 Unit: HOUR

IPSec Lifetime: 16 Unit: HOUR

Shared Key: ********************

Confirm Shared Key: ********************

9 Enter the value for the pre-shared key that you recorded in Step 4.

10 Click **Submit**.

11 Do one of the following steps:

If	Do
IPSec is enabled	Step 12
IPSec is disabled	Step 20

At a PC or workstation with a web browser

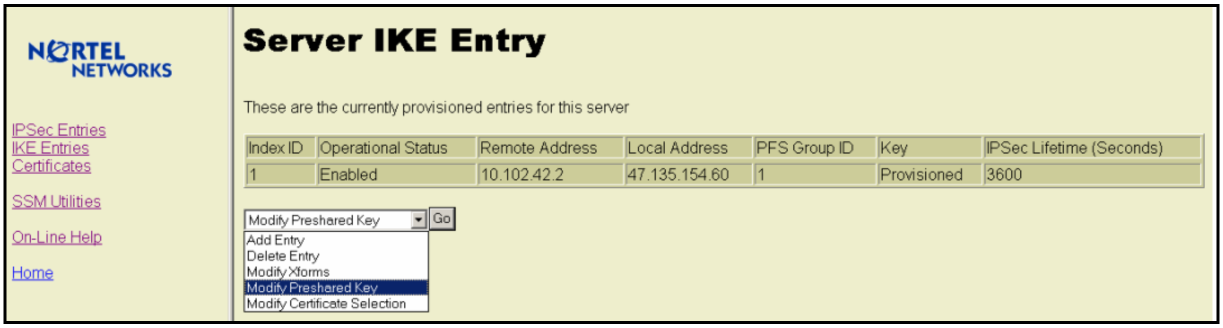
12 Launch the SSM.

13 Click the **IKE Entries** link on the SSM navigation bar.

The Server IKE Entries page appears.

14 From the menu, choose **Modify Pre-shared Key**.

Select IKE entry to modify page



Server IKE Entry

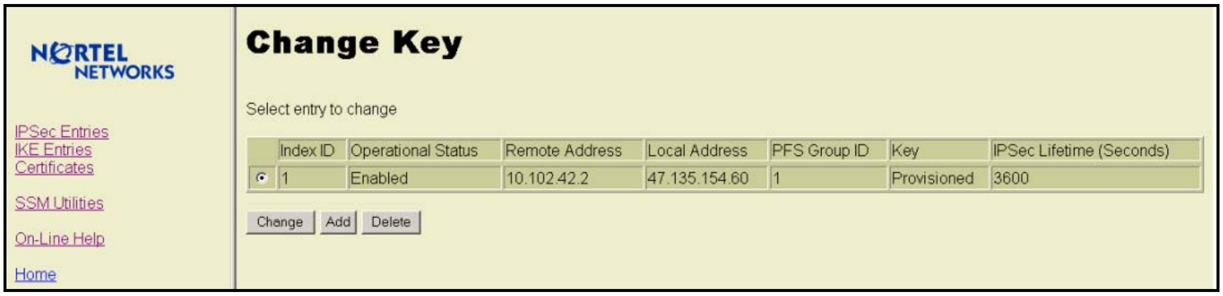
These are the currently provisioned entries for this server

Index ID	Operational Status	Remote Address	Local Address	PFS Group ID	Key	IPSec Lifetime (Seconds)
1	Enabled	10.102.42.2	47.135.154.60	1	Provisioned	3600

15 Click **Go**.

16 Select the entry representing the NE IP address that you recorded in Step 3 of this procedure.

Select IKE entry to modify page



Change Key

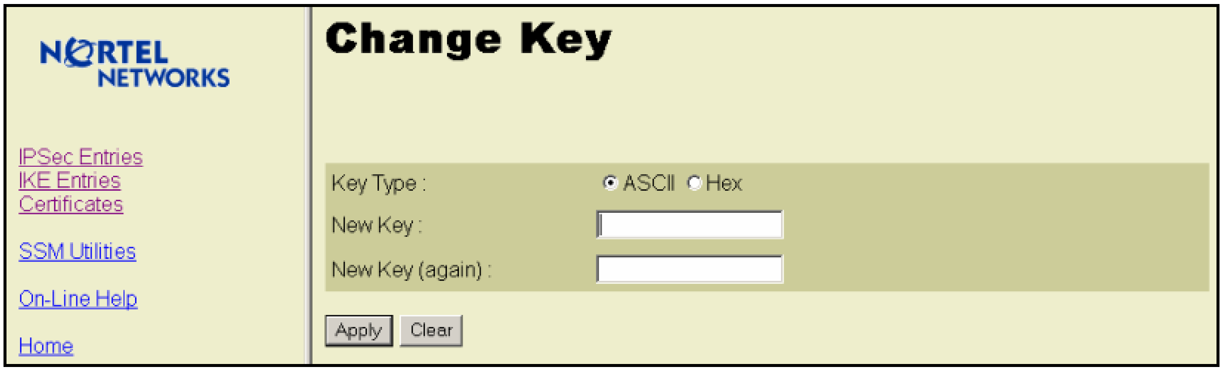
Select entry to change

	Index ID	Operational Status	Remote Address	Local Address	PFS Group ID	Key	IPSec Lifetime (Seconds)
●	1	Enabled	10.102.42.2	47.135.154.60	1	Provisioned	3600

17 Click **Change**.

The Change Key screen appears:

Changing the pre-shared key



Change Key

Key Type : ● ASCII ○ Hex

New Key :

New Key (again) :

18 Enter the value for the new key. The pre-shared key value you choose must be the same as that key used in Step 4.

> ***Note:*** If the encryption key entered at the SSM is incorrect and IPSec is enabled, a communication failure alarm (MGEM301) will occur.

19 Click **Apply**.

20 This procedure is complete.

Connection test tool

The connection test tool is accessed from the Subnet View using the Configuration menu. The connection test tool provide access to the ping and traceroute tools. The ping and traceroute tools can be used to verify the connection between the MG 9000 Manager server and the MG 9000. The tools can also be used during initial setup to verify connectivity if there is a communication failure. The connection test tool runs the ping or traceroute commands on the server and displays the results back to the client GUI.

The connection test tool can also be used to test the connectivity to the

- OAM&P CIPOA IP address, which is available by putting the cursor over the Subnet View and reading the IP address in the information balloon that appears
- GWC’s active IP address, which is available from the Switched Lines Services view in the GW Controller Config tab
- SAM21 shelf controllers, by obtaining the IP address from the SC Card View at the SAM21 GUI
- Nortel Networks Ethernet Routing Switch 8600 or Nortel Networks Multiservice Switch 15000 by obtaining the IP addresses from the network administrator

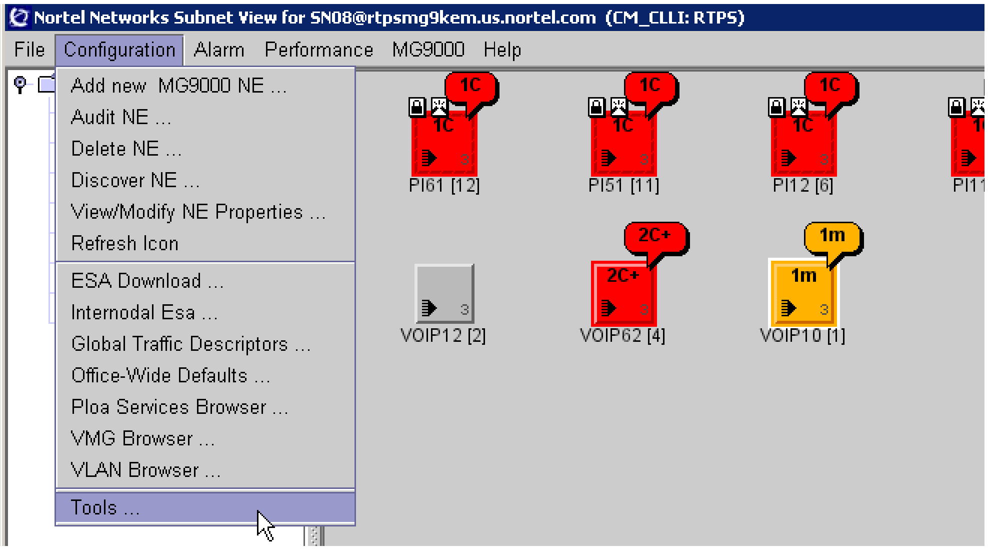
To access the connection test tools ping and traceroute, perform the following procedure.

Accessing the Connection test tool

At the MG 9000 Manager

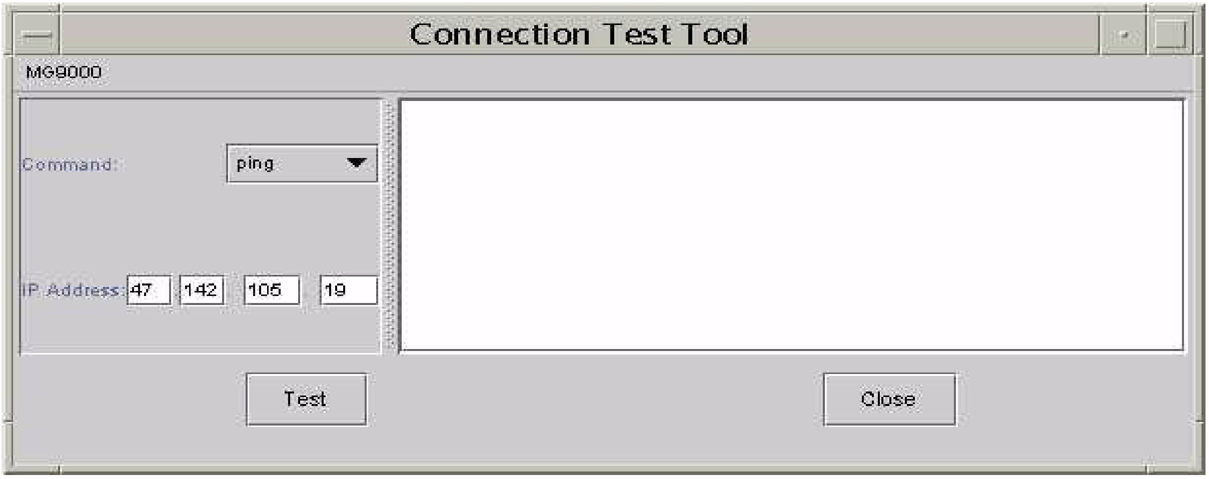
1 At the Subnet View, from the Configuration Menu, select Tools...as shown in the following figure.

Subnet View showing the Configuration menu



2 Select the command to be performed from the pull-down menu. The following figure shows the Connection Test Tool View and the Command pull-down menu.

Connection Test Tool View



Command: ping

IP Address: 47 142 105 19

3 Enter the IP address in the IP Address field.

> ***Note:*** The MG 9000 cannot be pinged until the MG 9000 has been commissioned with a cold start received by the MG 9000 Manager.

4 Click on Test to run the test tool. The results are displayed in the text area on the right.

5 This procedure is complete.

Starting a GUI client

At the MG 9000 Manager

1 Log into the GUI client workstation.

2 From a terminal, use the following UNIX command to stop the mid-tier server

```
<INSTALLDIR>/bin/mg9kclient
```

where <INSTALLDIR> is replaced with the directory path where the client was installed

3 This procedure is complete.

Stopping a GUI client

At the MG 9000 Manager

1 In the Subnet View, log out of the GUI client using the Exit menu item.

> ***Note:*** If the client does not respond to the Exit command, kill the GUI client by performing theKilling a UNIX process on the MG 9000 Manager.

2 This procedure is complete.

Restarting a GUI client

At the MG 9000 Manger

1 For the GUI client to be restarted, perform the Stopping a GUI client procedure and return to this step.

2 Perform the Starting a GUI client client procedure.

3 This procedure is complete.

Starting the mid-tier server

At the MG 9000 Manager

1 If the master servers have not been started, perform the Starting the master servers procedure

2 Log into the mid-tier workstation

3 From a terminal, use the following UNIX command to stop the mid-tier server

```
/opt/nortel/mg9kmtr/bin/mg9kmidtier start
```

4 This procedure is complete.

Stopping the mid-tier server

At the MG 9000 Manager

1 Perform the Stopping a GUI client procedure for all GUI clients and return to this step.

2 Log into the mid-tier server

3 From a terminal, use the following UNIX command to stop the mid-tier server

```
/opt/nortel/mg9kmtr/bin/mg9kmidtier stop
```

4 This procedure is complete.

Restarting the mid-tier server

At the MG 9000 Manager

1 Perform the Stopping the mid-tier server procedure and return to this step.

2 Perform the Starting the mid-tier server procedure and return to this step.

3 Perform the Starting a GUI client procedure for all GUI clients.

4 This procedure is complete.

Starting the master servers

At the MG 9000 Manager

1 Log into the master server workstation.

2 From a terminal, use the following UNIX command to start all the master server processing

```
/opt/nortel/mg9ksrv/bin/mg9kserver start
```

3 This procedure is complete.

Stopping the master servers

At the MG 9000 Manager

1 Perform the Stopping a GUI client procedure for all GUI clients and return to this step.

2 Perform the Stopping the mid-tier server procedure and return to this step.

3 Log into the master server workstation.

4 From a terminal, use the following UNIX command to stop all the master server processes

```
/opt/nortel/mg9ksrv/bin/mg9kserver stop
```

5 This procedure is complete.

Restarting the master servers

At the MG 9000 Manager

1 Perform the Stopping the master servers procedure and return to this step.

2 Perform the Starting the master servers procedure and return to this step.

3 Perform the Starting the mid-tier server procedure.

4 This procedure is complete.

When restarting the master server, use the following information to avoid data corruption and a mismatch of configuration data between the MG 9000, MG 9000 Manager, SESM, GWC, and Core:

When the MG 9000 Manager is restarted, it reads the data from the Oracle Database and audits the data contained in the MG 9000. If mismatches are found, it will correct them. To achieve this, all MG 9000 Manager data must be persisted. The MG 9000 Manager periodically initiates persistence of the MG 9000 Manager data in the Oracle database. The interval is set to 60 minutes. If configuration data changes were done during the last hour prior to restart, there is a possibility of data loss. This would include any line provisioning changes through OSSGate.

> ***Note:*** When restarting the MG 9000 Manager and recovering the PLoA Active or Passive end points, if the active end point is created with a remote ATM address matching the ATM address of a passive end point on the same subnet, then the active and passive services are converted to Full Private Line service.

To eliminate data loss, before the MG 9000 Manager is restarted, at the Subnet View:

- In the menu bar, click on MG9000->Persistence. The Persist data window appears and will list all nodes.
- Select one node at a time and click Apply to persist the latest copy of the data.

Starting the MG 9000 Manager

At the MG 9000 Manager

1 Perform the Starting the master servers procedure and return to this step.

2 Perform the Starting the mid-tier server procedure and return to this step.

3 Perform the Starting a GUI client procedure for all GUI clients.

4 This procedure is complete.

Stopping the MG 9000 Manager

At the MG 9000 Manager

1 Perform the Stopping the master servers procedure.

2 Perform the Stopping the mid-tier server procedure.

3 This procedure is complete.

Restarting the MG 9000 Manager

At the MG 9000 Manager

1 Perform the Stopping the MG 9000 Manager procedure and return to this step.

2 Perform the Starting the MG 9000 Manager procedure.

3 This procedure is complete.

Killing a UNIX process on the MG 9000 Manager

At the MG 9000 Manager

1 Log into the workstation where the process is running.

2 Enter the following command at the command line

```
ps -ef|grep java
```

The system returns a list of all processes running using the Java virtual machine with the last column in each row displaying an 80 character string that allows the startup command line option that the Java machine used to startup the process. The following is a sample output string:

```
/home/userid/nortel/mg9kem/jre/bin/../bin/spar
c/native_threads/java
-verbose:g -ms256msnm_FwComp.desktop.Desktop
```

Note: Only the first 80 characters of the command line will be displayed. Depending on where the client was installed, the string may be truncated.

3 Find the row in the output that corresponds to the process to kill. The second column of that row will display the UNIX ProcessID.

4 Enter the following UNIX command to terminate the process that is not responding

```
kill -KILL <PROCESS_ID>
```

where <PROCESS_ID> is the number in the second column of the output

5 This procedure is complete.

Shutting down the SPFS servers

When it is necessary to shut down the SPFS servers on which the MG 9000 master and mid-tier server software run, refer to procedure Shutting down an SPFS-based server in *ATM/IP Solution-Level Fault Management*, NN10408-900.

Clearing IP Security faults

Purpose of this procedure

This procedure describes the types of IP Security (IPSec) faults that can occur and the methods to recover from such faults.

The Nortel Carrier Voice over IP security service solution involves the interaction of several network elements. For information regarding the alarm clearing procedures for the MG 9000 and the MG 9000 Manager within the Carrier Voice over IP solution, you must refer to *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100.

> **CAUTION**
> **Risk of communication disruption, loss of service, or outage.**
> This procedure is provided for reference purposes only and is superseded by the procedures documented in *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100. You must use the procedures documented in *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100.

IPSec alarm clearing

The IPSC307 through IPSC313 treat digital certificate authentication alarms. These alarms indicate that an MG 9000 digital certificate has expired, is not valid or is otherwise corrupted. These alarms clear when a new digital certificate is successfully downloaded to the MG 9000.

The MG 9000 Element Manager (EM) will try to re-send the certificate when it receives an IPSC307-313 alarm from the gateway. The number of times the EM retries and the duration between the retries are configurable. When the retries are exhausted, manual intervention is required to download a valid certificate.

If the re-send failed because of download issues, there will be an EM alarm (IPSC314) indicating why it failed. If the re-send was successful, but the new certificate does not resolve the original issue in the gateway, the gateway cannot clear the original alarm (IPSC307-313). In such a case, the gateway does not re-send the alarm, and manual intervention is required to download a valid certificate.

When to use this procedure

Use this procedure when clearing IP Security faults.

Prerequisites

The procedure has no prerequisites.

Action

The following table lists the alarms generated for IP Security, the alarm severity, the log generated, and action to clear the alarm. For information on configuring IP Security, refer to *MG 9000 Security and Administration*, NN10162-511 and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

IP Security alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: ipsecMismatchSharedKey Severity: Critical Log: IPSC300	Cause: During negotiation, the key received did not match the one locally set. Action: Check for a mismatched key between the two nodes (MG 9000 to GWC or MG9000 to MG 9000 Manager). Reconfigure the key to clear this alarm. Refer to *MG 9000 Security and Administration*, NN10162-611 for information on configuring IPSec keys and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: ipsecikePeerLinkExpired Severity: Critical Log: IPSC301	Cause: Phase 1 security association has expired or is not present. Action: To clear this alarm, check the following: • communication link down. Check for other communication alarms. • IPSec parameter mismatch. Refer to *MG 9000 Security and Administration*, NN10162-611and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100 for information on configuring IPSec keys. • remote unit off line. Check for other alarms.

IP Security alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: ipsecSecureLinkExpired Severity: Critical Log: IPSC302	Cause: Phase 2 security association has expired or is not present. Action: Check the following: • communication link down. Check for other communication alarms. • IPSec parameter mismatch. Refer to *MG 9000 Security and Administration*, NN10162-611and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100 for information on configuring IPSec keys. • remote unit off line. Check for other alarms.
Type: ipsecDoSCallP Severity: Critical Log; IPSC303	Cause: Packets are being replayed to the call processing interface. Possible Denial of Service attack. Action: None, for information only. Clears when condition stops. Check customer logs for IP addresses from suspect packets. Determine if the IP addresses are valid and correct any possible configuration problems. Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: ipsecDoSMgmt Severity: Critical Log; IPSC304	Cause: Packets are being replayed to the call processing interface. Possible Denial of Service attack. Action: None, for information only. Clears when condition stops. Check customer logs for IP addresses from suspect packets. Determine if the IP addresses are valid and correct any possible configuration problems. Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

IP Security alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: ipsecMaxDiscardedPktRate Severity: Minor Log: IPSC305	Cause: An inordinate percentage of the received/transmitted packets are being discarded as a result of current security policies. Indicates a possible mis-configuration or denial of service attack. Action: None, for information only. Clears when condition stops. Check customer logs for IP addresses from suspect packets. Determine if the IP addresses are valid and correct any possible configuration problems. Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: ipsecRadiusTimeout Severity: Major Log: IPSC306	Cause: Requests from an MG 9000 sent to Radius server have timed out. Action: None, for information only. The remote unit may be off-line. Alarm clears when the connection resumes. Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: expiredLocalCertif Severity: Major Log: IPSC307	Cause: The IPSC digital certificate has expired. Action: Verify that the MG 9000 system clock is correct using procedure Querying and adjusting the MG 9000 system clock, then download a valid certificate using Downloading a valid certificate Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: certifExpiresIn4days Severity: Major Log: IPSC308	Cause: The IPSC digital certificate will expire in 4 days. Action: Verify that the MG 9000 system clock is correct using procedure Querying and adjusting the MG 9000 system clock, then download a new certificate using Downloading a valid certificate Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

IP Security alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: invalidFromDate Severity: Major Log: IPSC309	Cause: The IPSC digital certificate has an invalid from date. Action: Verify that the MG 9000 system clock is correct using procedure Querying and adjusting the MG 9000 system clock, then download a valid certificate using Downloading a valid certificate Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: noCertifInstalled Severity: Major Log: IPSC310	Cause: No certificate installed for the selected network element (NE) or virtual media gateway (VMG). Action: Configure TOD server and time zone, or set time and date and time zone. Download valid certificate. See the procedures Querying and adjusting the MG 9000 system clock then Downloading a valid certificate Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: remoteCertifVerifFailed Severity: Major Log: IPSC311	Cause: The remote certificate verification process has failed. Action: Information only. No action required. Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Type: missingSubjAltName Severity: Major Log: IPSC312	Cause: The IPSC digital certificate is missing the Subject Alt. Name. Action: Verify that the MG 9000 system clock is correct using procedure Querying and adjusting the MG 9000 system clock, then download a valid certificate using Downloading a valid certificate Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

IP Security alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: certificateFailure Severity: Major Log: IPSC313	Cause: A digital certificate has failed. Action: Verify that the MG 9000 system clock is correct using procedure Querying and adjusting the MG 9000 system clock, then download a valid certificate using Downloading a valid certificate Refer to *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

IP Security alarms

Alarm category, severity, and log report	Cause of alarm and action
Type: CertificateDownloadFault Severity: Major Log: IPSC314	Cause: The EM attempted, but failed, to deliver IPSec certificate to the gateway. Possible causes are: • Problem with physical IP network between the MG 9000 and MG 9000 EM, or between the MG 9000 EM and the IEMS. Action: Troubleshoot the IP connectivity (PING). • IP communication failure between the MG 9000 EM and the IEMS because of a problem with HTTPS. Action: If an error occurs while retrieving a certificate from the Certificate Manger, ensure that the Certificate Manager and the Certificate Manager Client are configured and working correctly.To do so, refer to the procedures on configuring the Certificate Manager, the entity default values, and the broker default values for the Certificate Manager in *IEMS Security and Administration*, NN10336-611 and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100. Check that valid WEBPKPROXY certificates are properly installed in the MG 9000 EM and the Certificate Manager. For procedures on how view the WEBPKPROXY certificates that have been installed, and to install WEBPKPROXY certificates using the generate and export function, see *IEMS Security and Administration*, NN10336-611and *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

Querying the MG 9000 system clock

When addressing alarms IPSPC307-311, and 313-314, you must first ensure that the Time server, or Time of Day and Time Zone has been configured correctly. If the time of day is not set correctly, the system can erroneously declare a digital certificate to have an invalid date. Use the following procedure to query, and if necessary adjust, the clock settings of an MG 9000. Additional details on Time of Day settings are available in *MG 9000 Configuration Management*, NN10096-511.

Querying and adjusting the MG 9000 system clock

At the LCI

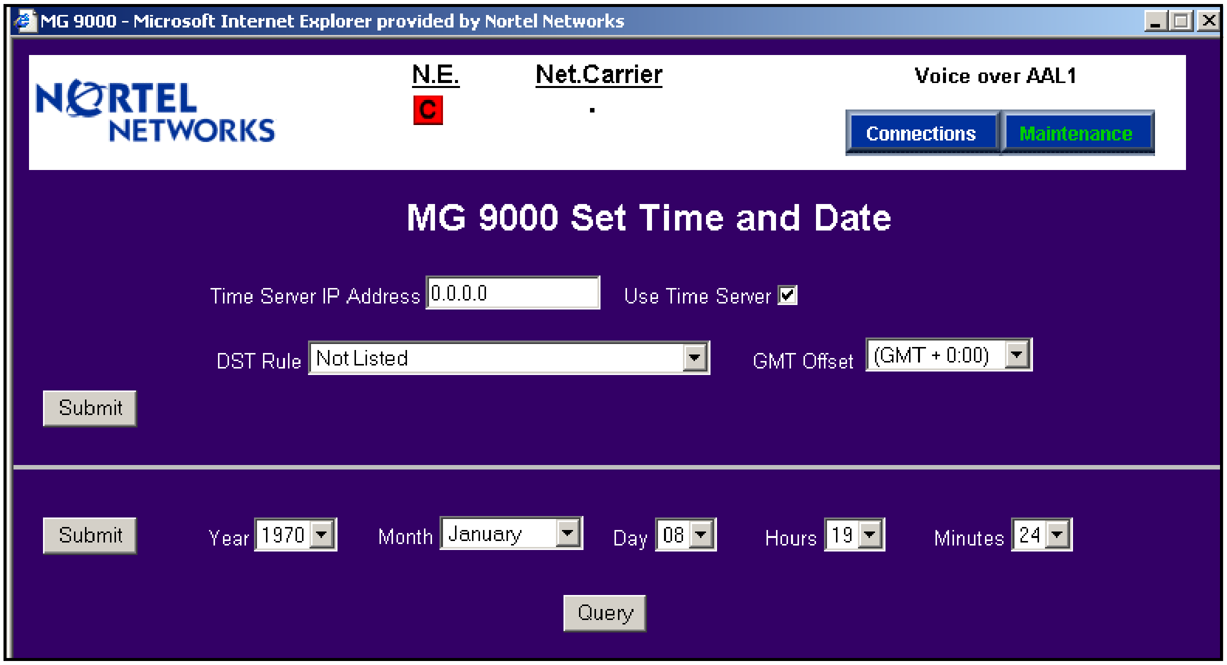
1 Click the **Connections** button.

The Connection Main Page opens.

2 From the navigation bar on the left side of the page, click **Time of Day**.

The MG 9000 Set Time and Date screen appears:

MG 9000 Set Time and Date screen



MG 9000 Set Time and Date

Time Server IP Address 0.0.0.0 Use Time Server ☑

DST Rule Not Listed GMT Offset (GMT + 0:00)

Year 1970 Month January Day 08 Hours 19 Minutes 24

3 Click **Query**.

The screen displays the current time settings.

If	Do
the time or time zone information is incorrect	go to Step 4
the time setting is correct	go to Step 7

4 Do one of the following.

If	Do
you use a time server	in the MG 9000 Set Time and Date screen, enter the IP address for your network time provider in the **Time Server IP Address** field and click on the **Use Time Server** box
a time server is not available	in the bottom portion of the MG 9000 Set Time and Date screen, set the current time and date

5 Set the time zone data by choosing the daylight savings time (DST) Rule and the Greenwich Mean Time (GMT) offset value which correspond to your geographical location.

6 Click **Submit**.

The system re-sets the MG 9000 system clock.

7 You have completed this procedure. You can proceed to troubleshoot the alarm.

Downloading a valid certificate

Use the following procedure to download a valid certificate.

CAUTION
Risk of communication disruption, loss of service, or outage.
This procedure is provided for reference purposes only and is superseded by the procedures documented in *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100. You must use the procedures documented in *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100.

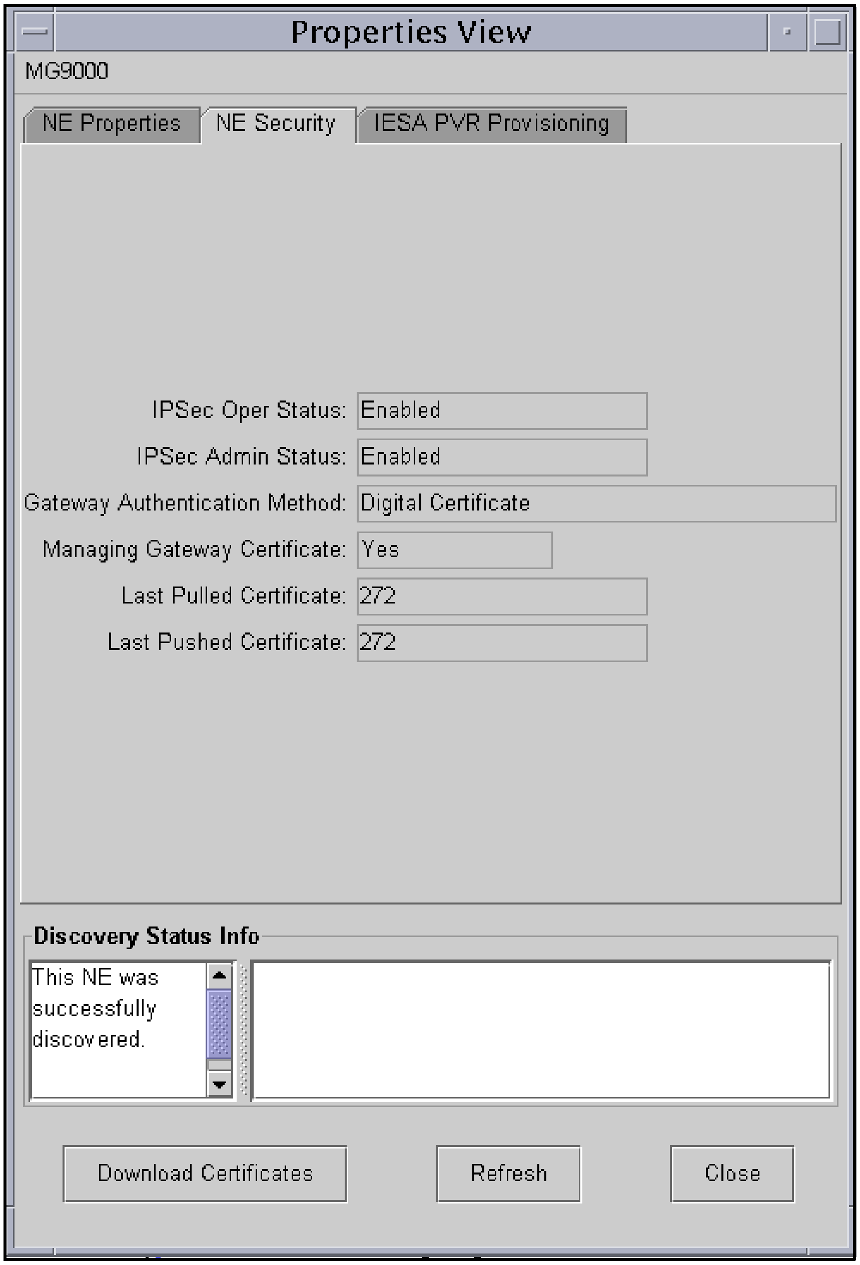
Downloading a valid certificate

At the MG 9000 Manager Subnet View

1 Choose a NE and select **Configuration > View/Modify NE Properties**. The Properties View appears.

2 Click the **NE Security** tab. The **NE Security** view appears:

Properties View showing the NE Security Properties View



IPSec Oper Status: Enabled

IPSec Admin Status: Enabled

Gateway Authentication Method: Digital Certificate

Managing Gateway Certificate: Yes

Last Pulled Certificate: 272

Last Pushed Certificate: 272

This NE was successfully discovered.

3 Click **Download Certificates** (this command requests and downloads a certificate to the MG 9000).

Watch the progress messages at the bottom of the GUI. The message indicates the success or failure of the MG 9000 EM to

- retrieve certificates from the IEMS
- download certificates to the MG 9000

4 You have completed this procedure.

Testing MG 9000 components

The following describe tests that can be run on MG 9000 equipment.

- Common equipment card diagnostics
- Line circuit diagnostics
- DS1 IMA link pattern test
- DS1 IMA carrier test
- Testing lines
- Operating line cut-off relay

Common equipment card diagnostics

Purpose of this procedure

The Card Diagnostic subsystem provides utilities that the Node and Card Maintenance subsystem uses to diagnose the intelligent MG 9000 cards. The utilities are implemented using lower level utilities provided by the logical device drivers (LDD) on the card.

Each diagnostic request has a priority of critical or normal. A critical diagnostic that arrives while a normal diagnostic is running preempts the normal diagnostic to halt and start again later. Critical diagnostics cannot preempt other critical diagnostics.

The following are the three different types of diagnostics:

- In-Service: This diagnostic has about 5% to 10% coverage.
- Out-Of-Service: This diagnostic has about 10% to 20% coverage.
- Severely Destructive: This diagnostic has about 30% to 90% coverage (interrupts links to other cards and external to the MG 9000). These diagnostic tests are service affecting and will drop active calls and should only be performed during low traffic periods.

> ***Note:*** The severely destructive diagnostic appears as an option in the Diagnostics View, but is currently disabled.

The following are the common equipment card diagnostic procedures.

- Performing in-service diagnostics on common equipment cards
- Performing out-of-service diagnostics on common equipment cards
- Querying common equipment diagnostics
- Aborting diagnostics on common equipment cards

When to use this procedure

Use these procedures to perform in-service or out-of-service diagnostics on common equipment cards, which includes the DCC, ITP, ITX, ABI, and DS1 cards.

Prerequisites

These procedures have no prerequisites.

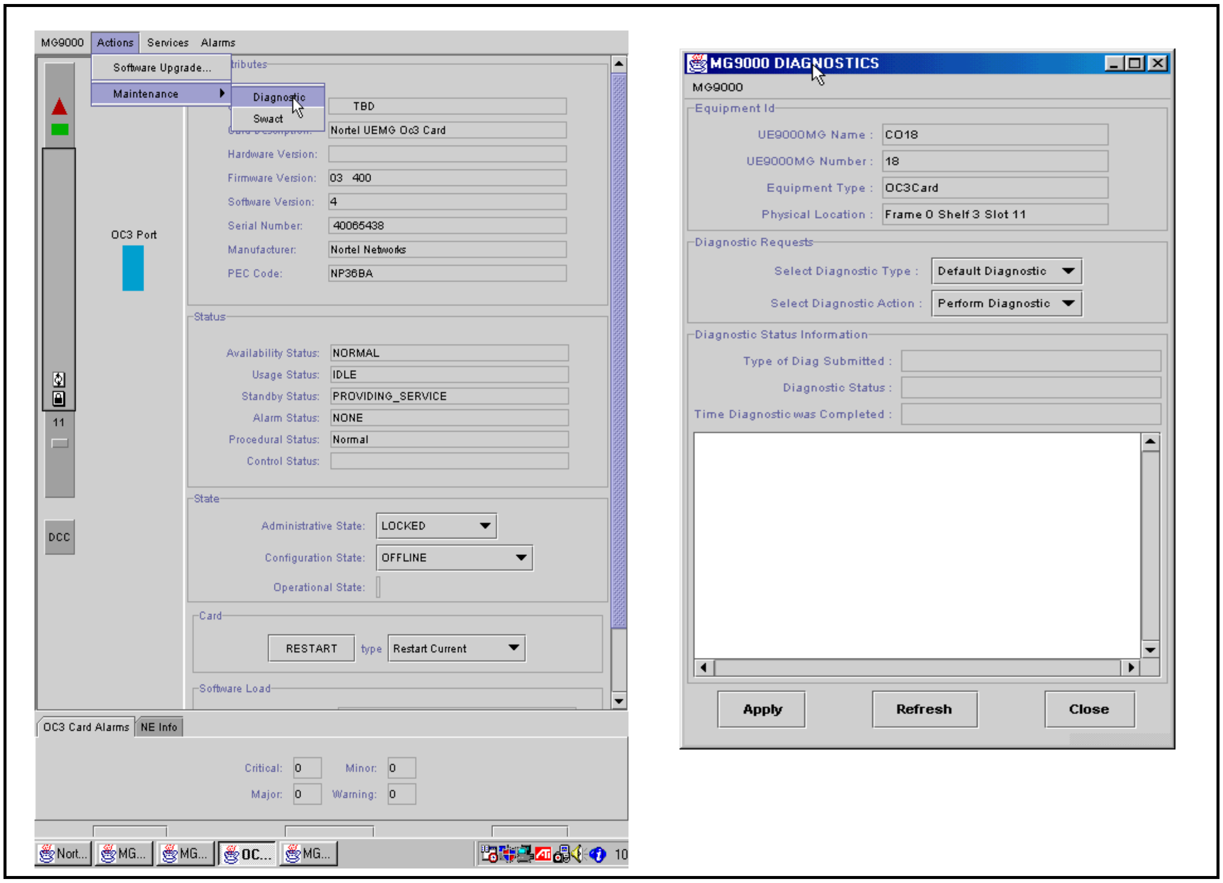
Action

Performing in-service diagnostics on common equipment cards

At the MG 9000 Manager

1. At the Subnet View, select the MG 9000 on which diagnostics are to be performed. The Frame View appears.
2. Double click on the shelf to open the Shelf View.
3. Double click on the card on which diagnostics are to be run. The Card View appears.
4. Verify that the administrative state of the card is set to unlocked. To Unlock the card, perform the Unlocking a card procedure.
5. From the menu bar on the top left of the Card View, select Actions->Maintenance->Diagnostic as shown in the following figure. The following MG 9000 Diagnostics View appears.

Card View and MG 9000 Diagnostic View



TBD
Card Description: Nortel UEMG Oc3 Card
Hardware Version:
Firmware Version: 03 400
Software Version: 4
Serial Number: 40065438
Manufacturer: Nortel Networks
PEC Code: NP36BA

Status
Availability Status: NORMAL
Usage Status: IDLE
Standby Status: PROVIDING_SERVICE
Alarm Status: NONE
Procedural Status: Normal
Control Status:

State
Administrative State: LOCKED
Configuration State: OFFLINE
Operational State:

Card
type: Restart Current

Software Load

Critical: 0 Minor: 0
Major: 0 Warning: 0

MG9000 DIAGNOSTICS
MG9000
Equipment Id
UE9000MG Name : CO18
UE9000MG Number : 18
Equipment Type : OC3Card
Physical Location : Frame 0 Shelf 3 Slot 11

Diagnostic Requests
Select Diagnostic Type : Default Diagnostic
Select Diagnostic Action : Perform Diagnostic

Diagnostic Status Information
Type of Diag Submitted :
Diagnostic Status :
Time Diagnostic was Completed :

6. Select the Default Diagnostic in the Select Diagnostic Type field.

7 Select Perform Diagnostic in the Select Diagnostic Type field.

> ***Note:*** Normally this field is initially set to Perform Diagnostic. If the field is already set to Perform Diagnostic, go to step 8.

8 Click the Apply button at the bottom of the Diagnostic View.

9 This procedure is complete.

Performing out-of-service diagnostics on common equipment cards

At the MG 9000 Manager

1 At the Subnet View, select the MG 9000 on which diagnostics are to be performed. The Frame View appears.

2 Double click on the shelf to open the Shelf View.

3 Double click on the card on which diagnostics are to be run. The Card View appears.

4 Verify that the administrative state of the card is set to locked. To lock the card, perform the Locking a card procedure.

5 Select the Default Diagnostic in the Select Diagnostic Type field.

6 Select Perform Diagnostic in the Select Diagnostic Type field.

> ***Note:*** Normally this field is initially set to Perform Diagnostic. If the field is already set to Perform Diagnostic, go to step 7.

7 Click the Apply button at the bottom of the Diagnostic View.

8 This procedure is complete.

Query common equipment diagnostics

Purpose of this procedure

This procedure provides a series of steps to query in-service, out-of-service, and destructive diagnostics on common equipment.

When to use this procedure

Use these procedures when it is necessary to query in-service or out-of-service common equipment diagnostics.

Prerequisites

A common equipment diagnostic is run.

Action

Querying common equipment diagnostics

At the Diagnostics View

1 Determine if a Default Diagnostic or Destructive Diagnostic is in progress by performing the following steps:

a Check to see if the Type of Diag Submitted field is set to Default Diagnostic or Destructive Diagnostic.

b Verify that the Diagnostic Status Field is set to In Progress.

2 Select Query Diagnostic in the Select Diagnostic Actions field.

3 Click the Apply button at the bottom of the Diagnostic View.

4 This procedure is complete.

Aborting diagnostics on common equipment

Purpose of this procedure

Use this procedure to abort in-service, out-of-service, and destructive diagnostics on common equipment cards.

When to use this procedure

Use these procedures when it is necessary to abort in-service or out-of-service common equipment diagnostics.

Prerequisites

The MG 9000 must be executing common equipment diagnostics. Refer to Performing in-service diagnostics on common equipment cards or Performing out-of-service diagnostics on common equipment cards.

Action

Aborting diagnostics on common equipment cards

At the MG 9000 Manager

1 At the Subnet View, select the MG 9000 on which diagnostics are running. The Frame View appears.

2 Double click on the shelf to open the Shelf View.

3 Double click on the card on which diagnostics are running. The Card View appears.

4 Determine if a Default Diagnostic or Destructive Diagnostic is in progress by performing the following steps:

- **a** Check to see if the Type of Diag Submitted field is set to Default Diagnostic or Destructive Diagnostic.
- **b** Verify that the Diagnostic Status Field is set to In Progress.

5 Select the Abort Diagnostic in the Select Diagnostic Actions field.

6 Click the Apply button at the bottom of the Diagnostic View.

7 This procedure is complete.

Marking a faulty circuit

Purpose of this procedure

This procedure describes the steps required to mark a line circuit (port) as faulty. This procedure applies to the following cards:

- World line card (WLC)
- Global line card (GLC)
- Digital subscriber line xDSL (Voice circuits only. XDSL data circuits cannot be marked as faulty.)
- Service Adapter Access (SAA)

When to use this procedure

Use this procedure to manually designate a circuit as faulty.

Prerequisites

The circuit must be in the locked state. If the circuit is in the unlocked state, the fault setting option on the GUI is disabled.

EWSMTC-level authorization is required to perform this procedure.

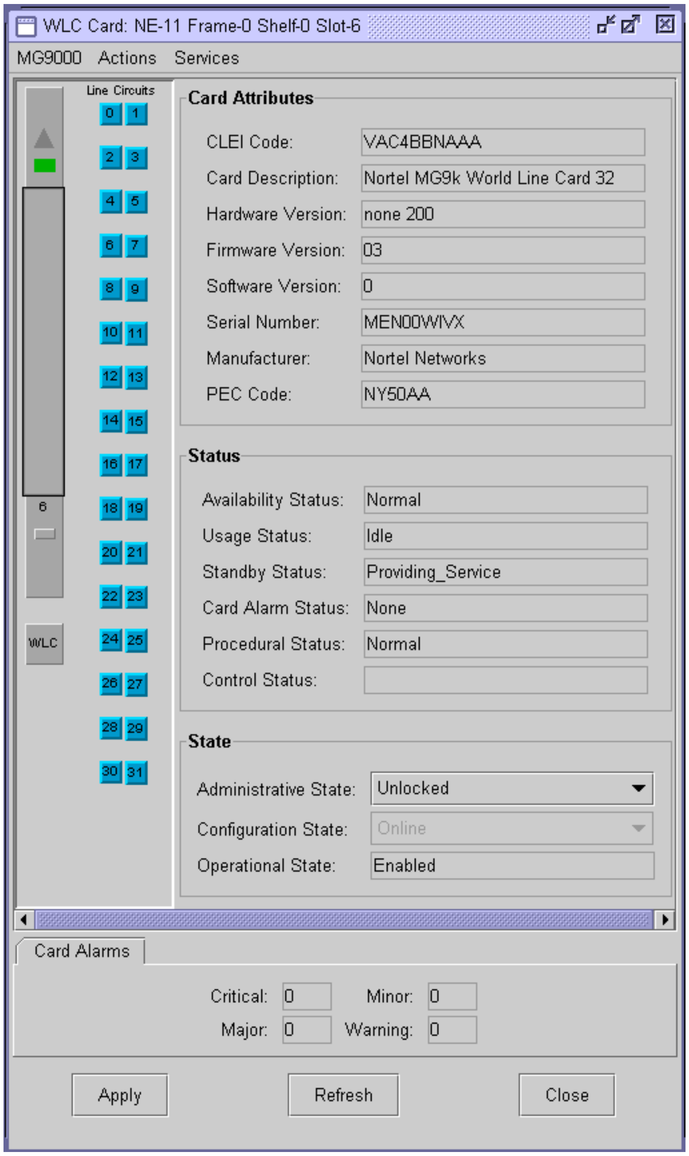
Action

Mark a faulty circuit using the following steps:

At the MG9000 Manager

1 At the Line card view, select the circuit that you want to mark as faulty.

WLC Line card view



Card Attributes

CLEI Code: VAC4BBNAAA
Card Description: Nortel MG9k World Line Card 32
Hardware Version: none 200
Firmware Version: 03
Software Version: 0
Serial Number: MEN00WIVX
Manufacturer: Nortel Networks
PEC Code: NY50AA

Status

Availability Status: Normal
Usage Status: Idle
Standby Status: Providing_Service
Card Alarm Status: None
Procedural Status: Normal
Control Status:

State

Administrative State: Unlocked
Configuration State: Online
Operational State: Enabled

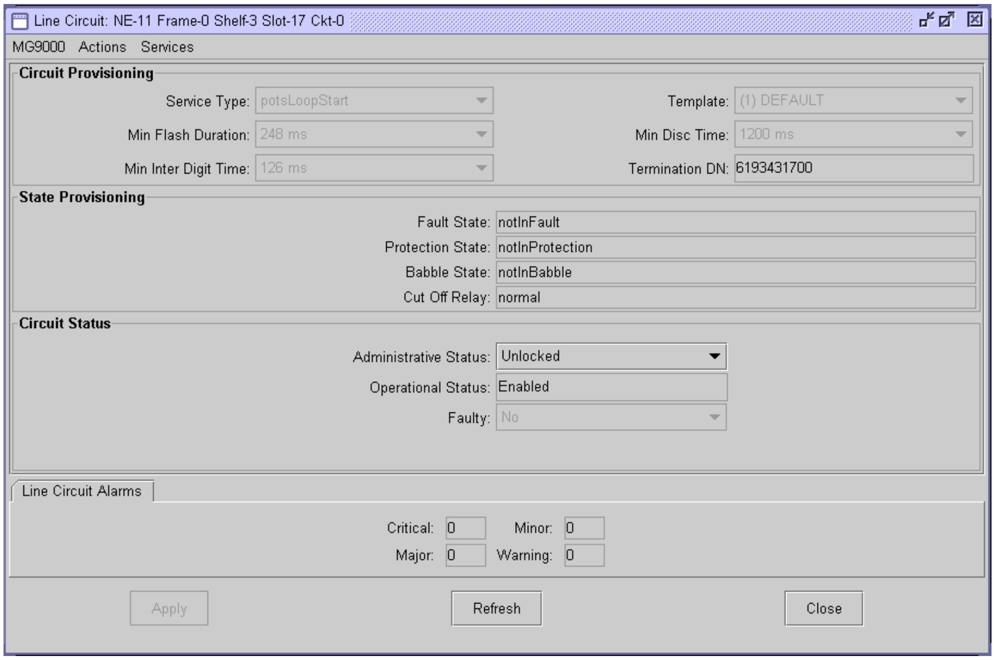
Card Alarms

Critical: 0 Minor: 0
Major: 0 Warning: 0

T*he Line Circuit view opens.*

2 In the Circuit Status area of the Line Circuit view, open the Faulty menu and select either "Yes" or "No".

WLC Line Circuit view



Line Circuit: NE-11 Frame-0 Shelf-3 Slot-17 Ckt-0

Circuit Provisioning

Service Type:	potsLoopStart	Template:	(1) DEFAULT
Min Flash Duration:	248 ms	Min Disc Time:	1200 ms
Min Inter Digit Time:	126 ms	Termination DN:	6193431700

State Provisioning

Fault State: notInFault
Protection State: notInProtection
Babble State: notInBabble
Cut Off Relay: normal

Circuit Status

Administrative Status: Unlocked
Operational Status: Enabled
Faulty: No

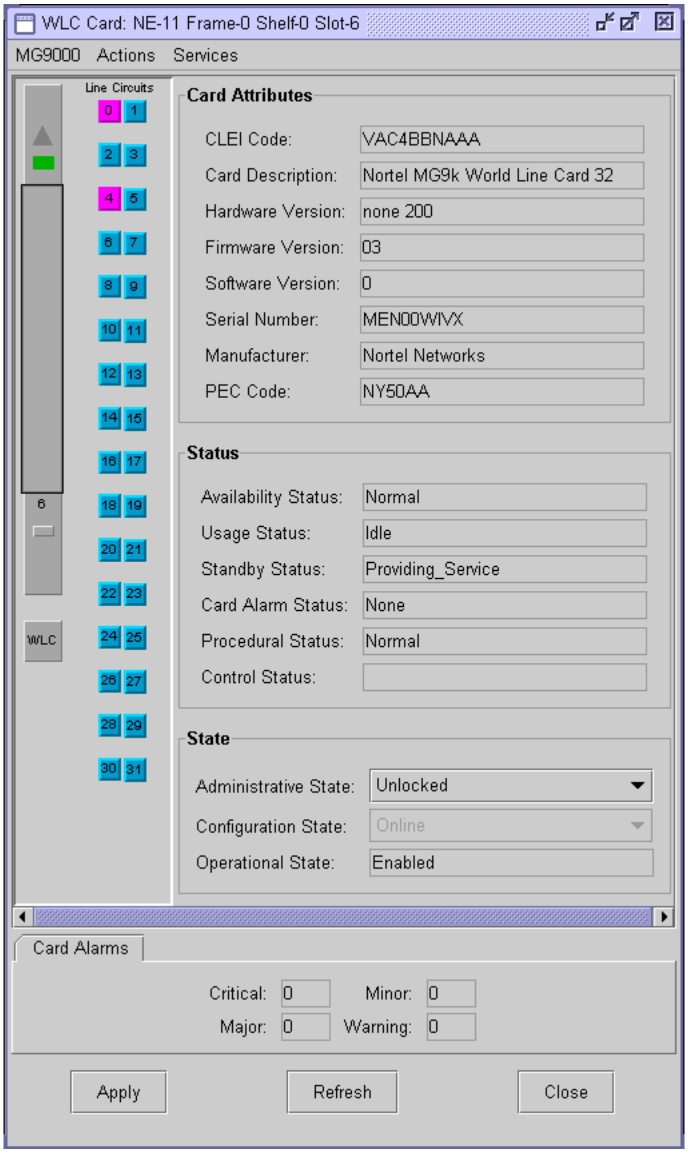
Line Circuit Alarms

Critical:	0	Minor:	0
Major:	0	Warning:	0

Note: You do not need to click Apply to change the Faulty status.

If a card is marked as faulty, it appears in the Line Card view in the color magenta, to distinguish it from in-service (blue) or alarm (red, orange, yellow) states, as shown in the following figure.

WLC Line Card View showing faulty circuits



Card Attributes

CLEI Code: VAC4BBNAAA

Card Description: Nortel MG9k World Line Card 32

Hardware Version: none 200

Firmware Version: 03

Software Version: 0

Serial Number: MEN00WIVX

Manufacturer: Nortel Networks

PEC Code: NY50AA

Status

Availability Status: Normal

Usage Status: Idle

Standby Status: Providing_Service

Card Alarm Status: None

Procedural Status: Normal

Control Status:

State

Administrative State: Unlocked

Configuration State: Online

Operational State: Enabled

Card Alarms

Critical: 0 Minor: 0

Major: 0 Warning: 0

> ***Note:*** The Faulty menu is enabled only when the Administrative Status is in the Locked state. For additional information, see the procedure Marking a faulty circuit on page 279.

3 This procedure is complete. To view a list of faulty circuits, see the procedure Marking a faulty circuit on page 279.

Viewing a list of faulty circuits

Purpose of this procedure

This procedure describes the steps required to access and view a list of faulty line circuits (ports).

This procedure applies to circuits on the following line cards:

- WLC
- GLC
- xDSL (voice circuits only)
- SAA

Faulty circuits are listed in the Faulty Circuit Listing view. This view is for information purposes only (read-only) and is intended to allow users to identify, isolate, and track faulty line circuits on a network element (NE).

When to use this procedure

Use this procedure to view a list of faulty line circuits.

Prerequisites

None.

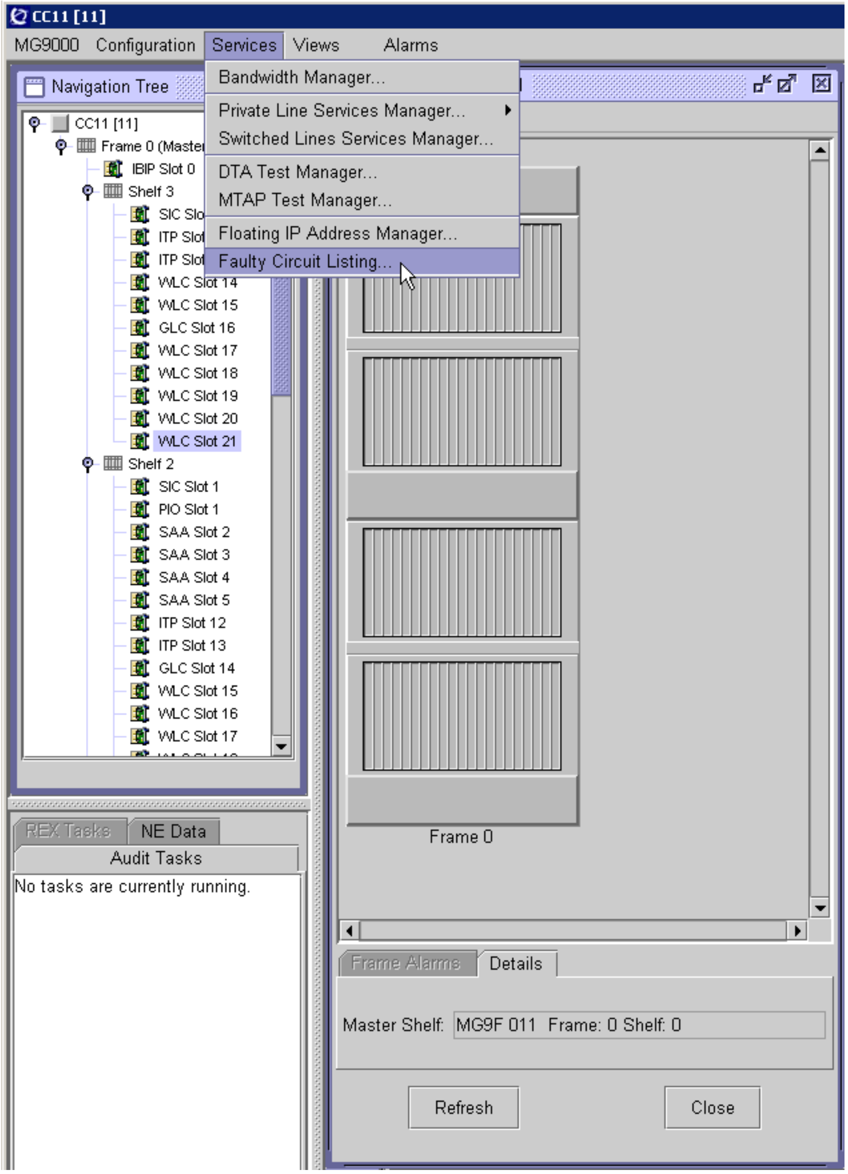
Action

View a list of faulty circuits using the following steps:

At the MG9000 Manager

1 At the **NE desktop** view, open the **Services** Menu.

Services Menu list



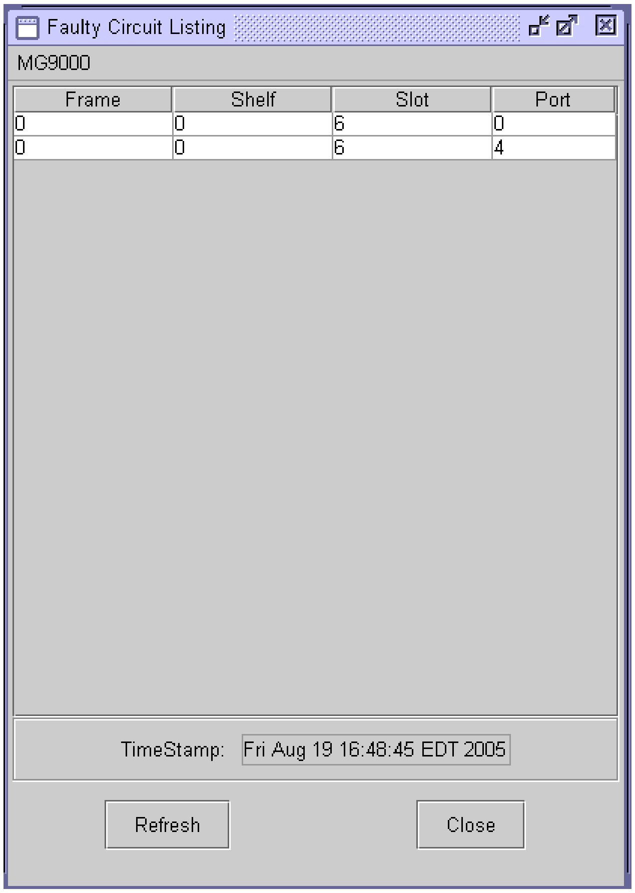
No tasks are currently running.

Master Shelf: MG9F 011 Frame: 0 Shelf: 0

2 Select the Faulty Circuit Listing menu item.

The Faulty Circuit Listing view appears.

Faulty Circuit Listing view



MG9000

Frame	Shelf	Slot	Port
0	0	6	0
0	0	6	4

TimeStamp: Fri Aug 19 16:48:45 EDT 2005

The Faulty Circuit Listing has the following fields:

- Frame Number
- Shelf Number
- Slot Number
- Port Number

3 Locate the time stamp at the bottom of the view.

The time stamp indicates the last time the data was synchronized with the database.

This view is not automatically updated. If the list is not current, click **Refresh** to view the latest information.

4 This procedure is complete.

Line circuit diagnostics

Purpose of this procedure

The Line Circuit Diagnostic subsystem provides utilities that perform diagnostics on line circuits connected to the following cards:

- World line card circuits (POTS 32 card)
- Global line card circuits (GLC 32 and GLC 12 cards)
- Service Adaptive Access circuits (SAA card) (not used in the UA-IP solution)
- Digital Subscriber Loop Voice and Data circuits (xDSL)

The following are the two types of supported Line Circuit diagnostics:

- In-Service: This diagnostic has about 5% to 10% coverage.
- Out-Of-Service: This diagnostic has about 10% to 20% coverage.

The following are the common equipment card diagnostic procedures.

- Performing in-service line diagnostics
- Performing out-of-service line diagnostics
- Query in-service and out-of-service line diagnostics
- Aborting line circuits diagnostics
- GLC circuit controller diagnostics

When to use this procedure

Use these procedures when it is necessary to perform in-service or out-of-service line diagnostics.

Prerequisites

These procedures have no prerequisites.

Action

Performing in-service line diagnostics

At the MG 9000 Manager

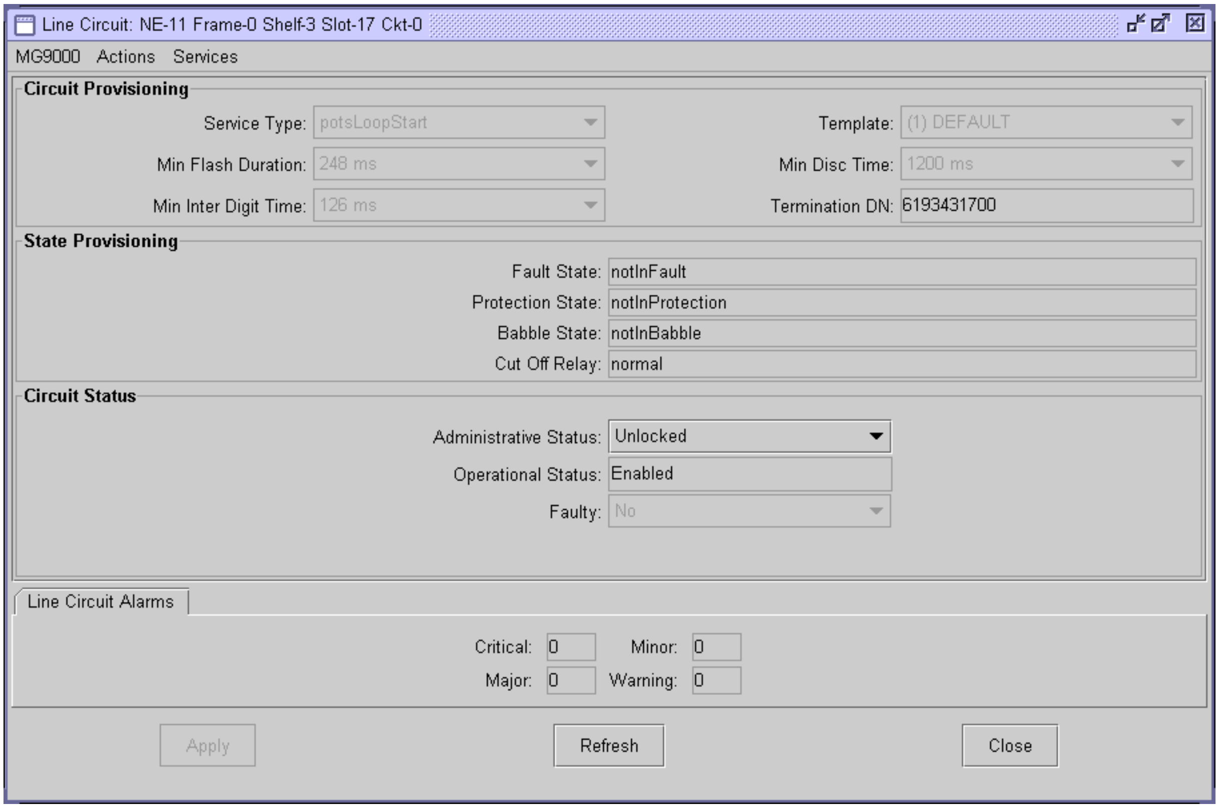
1 At the Subnet View, double click the MG 9000 icon on which diagnostics are to be run. The Frame View appears.

2 In the Frame View, double click on the shelf on which the circuits resides to be tested. The Shelf View appears.

3 In the Shelf View, double-click on the World Line card (POTS 32), GLC 32 card, SAA card, or xDSL card on which the diagnostics are to be run.

4 In the left side of the Card View, double-click on the circuit to be tested. The following screen appears.

Circuit View screen



Line Circuit: NE-11 Frame-0 Shelf-3 Slot-17 Ckt-0

Circuit Provisioning

Service Type: potsLoopStart

Template: (1) DEFAULT

Min Flash Duration: 248 ms

Min Disc Time: 1200 ms

Min Inter Digit Time: 126 ms

Termination DN: 6193431700

State Provisioning

Fault State: notInFault

Protection State: notInProtection

Babble State: notInBabble

Cut Off Relay: normal

Circuit Status

Administrative Status: Unlocked

Operational Status: Enabled

Faulty: No

Critical: 0 Minor: 0

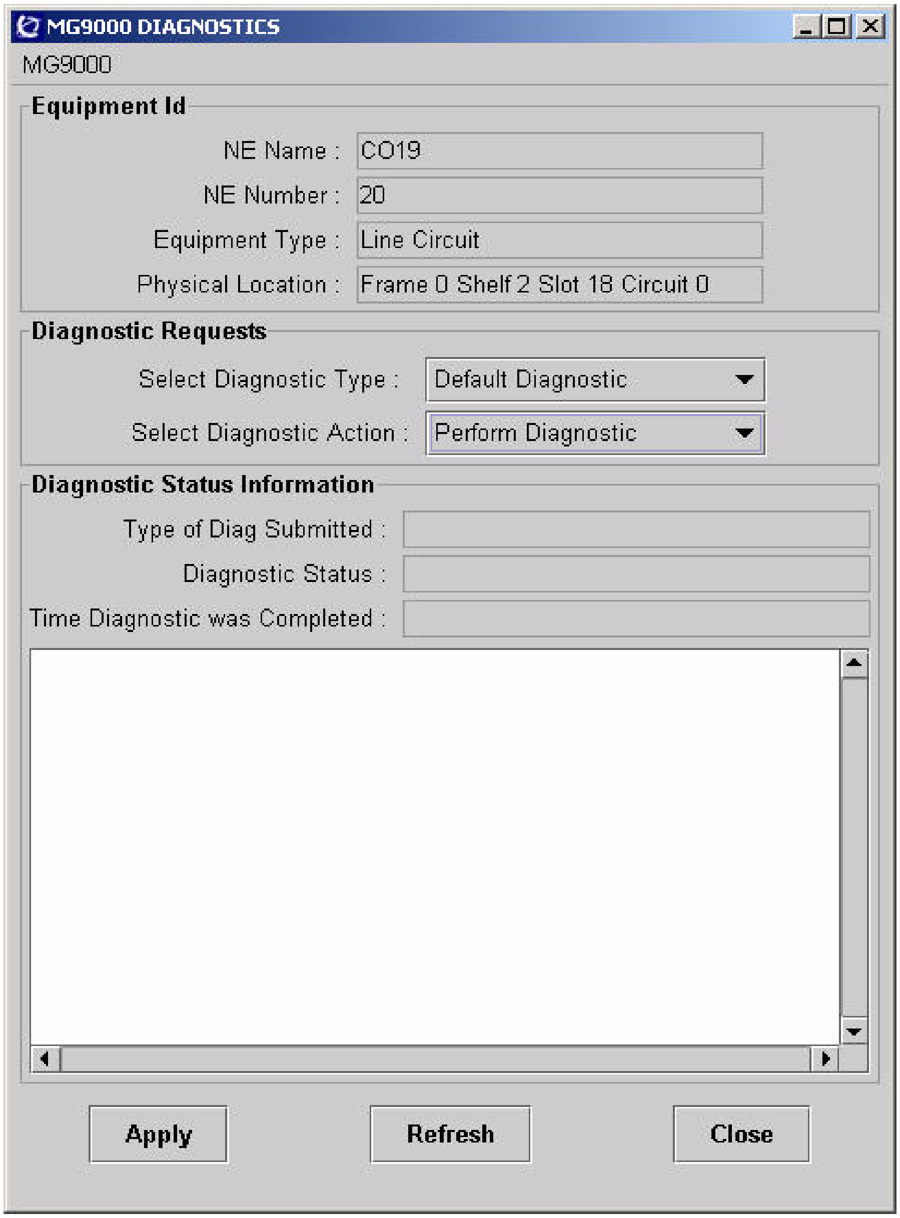
Major: 0 Warning: 0

5 Verify that the administrative state of the circuit is set to unlocked. If the card needs to be unlocked, in the Circuit status pane, select the Administrative status menu and select Unlocked. Otherwise, proceed to step 6.

> ***Note:*** If you attempt to unlock a circuit that is marked as faulty, the following message appears: "The circuit is marked as faulty. The existing service may be degraded. Are you sure?"
>
> Select "OK" to submit the unlock request to the gateway or select "Cancel."

6 From the Actions menu at the top of the screen, select Maintenance->Diagnostic. The following Diagnostic View screen appears.

Diagnostic View



NE Name : CO19

NE Number : 20

Equipment Type : Line Circuit

Physical Location : Frame 0 Shelf 2 Slot 18 Circuit 0

Select Diagnostic Type : Default Diagnostic

Select Diagnostic Action : Perform Diagnostic

Type of Diag Submitted :

Diagnostic Status :

Time Diagnostic was Completed :

The following table describes the fields in the Diagnostic View window.

Diagnostic View fields

Field	Explanation
NE Name	The name of the fully discovered network element.
NE Number	The number of the fully discovered network element.

Diagnostic View fields

Field	Explanation
Equipment Type	The name of the Equipment you are about to perform a diagnostic on.
Physical Location	The physical location of the equipment you are about to perform the diagnostic on.
Diagnostic Requests	Select Diagnostic Types - For the WLC Circuits, GLC 32 Circuits, SAA Circuits (service type is not P-phone), and the XDSL Voice Circuits, the available diagnostic types are Default Diagnostic; Test All; Off Hook Diagnostic; On Hook Diagnostic; Single Party Ringing Diagnostic; Coin Collect Diagnostic; Coin Return Diagnostic; Reverse Battery Diagnostic. For SAA circuits, if service type is P-phone, the available diagnostic type is Default Diagnostic. GLC cards NTNY53AA/BA/CA offer a Circuit Controller Diagnostic. The Circuit Controller Diagnostic determines if a circuit controller needs to be reloaded and it performs a reload when required. When a diagnostic is started on one of the circuits, the Select Diagnostic Types field is disabled and the user is not able to select another diagnostic type until the diagnostic is completed or aborted.

Diagnostic View fields

Field	Explanation
	Select Diagnostic Actions - There are three diagnostic actions a user can perform: Perform Diagnostic - initiates a diagnostic when the Apply button is pressed. • Query Diagnostic - retrieves the status of a diagnostic in progress • Abort Diagnostic - terminates the diagnostic in progress If there is no diagnostic in progress the Select Diagnostic Actions field contains the Perform Diagnostic option only. When the user initiates a diagnostic, the Perform Diagnostic option is removed and the Query Diagnostic and Abort Diagnostic options are available in the Select Diagnostic Actions field. When the diagnostic is completed or aborted, the Abort Diagnostic and Query Diagnostic options are removed and the Perform Diagnostic option is available again. The diagnostics normally occur very quickly therefore it may be difficult to either query or abort a diagnostic. The Query Diagnostic and Abort Diagnostic functions are fail-safe functions. The functions are useful when a diagnostic takes longer than normally expected or the MG 9000 Manager does not receive notification that the diagnostic has finished. In these cases, the user can either query the diagnostic that is in progress to check the status of the diagnostic or abort the diagnostic in progress.
Diagnostic Status Information	Type of Diag Submitted - The type of diagnostic submitted by user.

Diagnostic View fields

Field	Explanation
	Diagnostic Status - The status of the diagnostic. Possible values are: NONE, SUCCESS, INPROGRESS, NOTSUPPORTED, UNABLETORUN, ABORTED, FAILED. ***Note:*** When encountering multiple line card diagnostic failures, verify that the cable between the MTA card and the SIC card is correctly connected. If the cable is unplugged or loose, the line test system displays the result as `<individual diagnostic> fail` while if the Test All diag is performed, the line test system displays the result as `offhook all`. Time Diagnostic was Completed - The time the diagnostic was completed. The open text box at the bottom of the Diagnostic View displays whether the diagnostic passed or failed and additional diagnostic information.

7 Select one Diagnostic in the Select Diagnostic Type field.

8 Select Perform Diagnostic in the Select Diagnostic Action field.

Note: Normally this field is initially set to Perform Diagnostic. If the field is already set to Perform Diagnostic, go to step 9.

9 Click the Apply button at the bottom of the Diagnostic View.

10 This procedure is complete.

Performing out-of-service line diagnostics

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon on which diagnostics are to be run. The Frame View appears.

2 In the Frame View, double click on the shelf on which the circuits resides to be tested. The Shelf View appears.

3 In the Shelf View, double click on the World Line card (POTS 32), SAA card, or xDSL card on which the diagnostics are to be run.

4 In the left side of the Card View, double click on the circuit to be tested. The Circuit View screen appears.

5 From the Actions menu at the top of the screen, select Maintenance->Diagnostic. The Diagnostic View screen appears.

6 At the Diagnostic View for the selected circuit, verify that the Administrative state of the card is set to Locked. If the card needs to be locked, in the Circuit status pane, select the Administrative status pull down and select Locked. Otherwise proceed to step 7.

7 Select one Diagnostic in the Select Diagnostic Type field.

8 Select Perform Diagnostic in the Select Diagnostic Type field.

> ***Note:*** Normally this field is initially set to Perform Diagnostic. If the field is already set to Perform Diagnostic, go to step 9.

9 Click the Apply button at the bottom of the Diagnostic View.

10 This procedure is complete.

Query line circuit diagnostics

Purpose of this procedure

Use the following procedure to query in-service and out-of-service diagnostics on line circuits connected to the following cards:

- World line card circuits (POTS 32 card)
- Global line card circuits (GLC 32 card)
- Service Adaptive Access circuits (SAA card) (not used in the UA-IP solution)
- Digital Subscriber Loop Voice and Data circuits (xDSL)

When to use this procedure

Use this procedure when it is necessary to query in-service or out-of-service line diagnostics.

Prerequisites

A line circuit diagnostic is run.

Action

Query in-service and out-of-service line diagnostics

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon on which diagnostics are to be queried. The Frame View appears.

2 In the Frame View, double click on the shelf on which the circuits resides to be tested. The Shelf View appears.

3 In the Shelf View, double click on the World Line card (POTS 32), GLC 32 card, SAA card, or xDSL card on which the diagnostics are to be queried.

4 In the left side of the Card View, double click on the circuit under test. The Circuit View screen appears.

5 From the Actions menu at the top of the screen, select Maintenance->Diagnostic. The MG 9000 Diagnostic View appears.

6 Determine if a Default Diagnostic is in progress by performing the following steps:

a Check to see if the Type of Diag Submitted field is set to Default Diagnostic.

b Verify that the Diagnostic Status Field is set to InProgress.

7 Select Query Diagnostic in the Select Diagnostic Actions field.

8 Click the Apply button at the bottom of the Diagnostic View.

9 This procedure is complete.

GLC circuit controller diagnostics

Purpose of this procedure

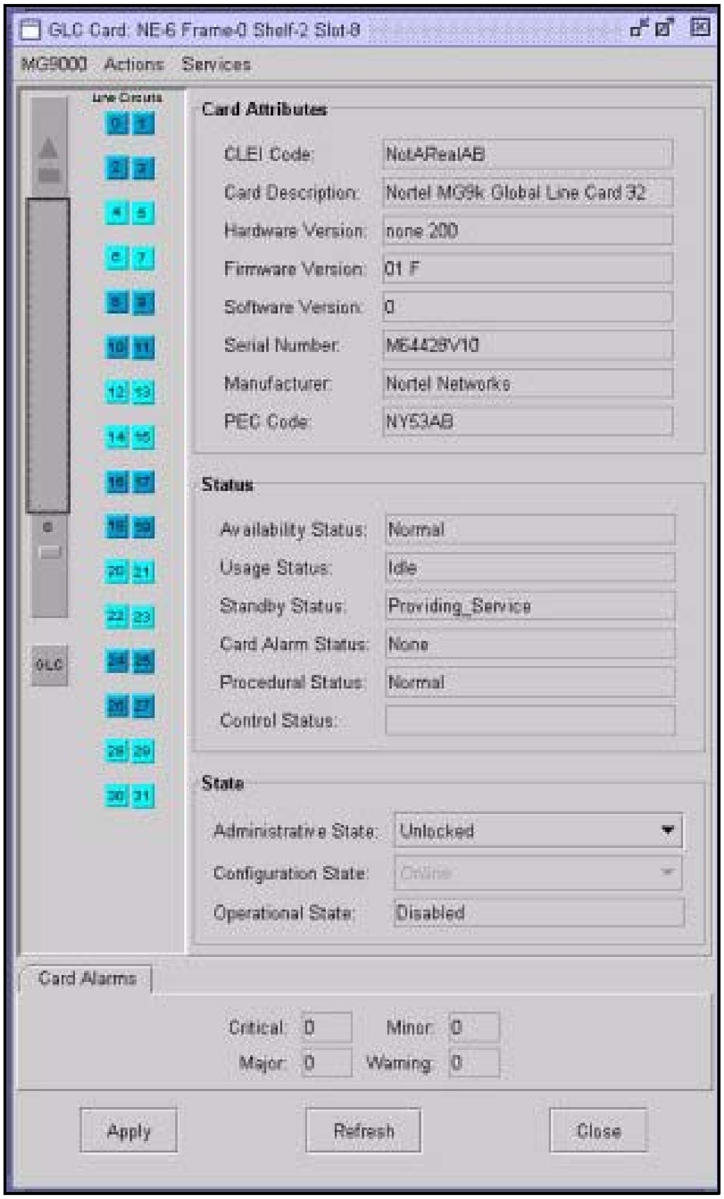
The Circuit Controller diagnostic is designed to determine if an individual circuit controller needs to be reloaded. This utility allows you to reload a single circuit controller from the MG 9000 Element Manager.

GLC 32 cards have 8 circuit controllers. GLC 12 cards have 3 circuit controllers. A single circuit controller controls 4 GLC line circuits at a time. If a single circuit controller is reloaded, call processing on the 4 GLC line circuits is dropped during a circuit controller reload. If the circuit controller does not need to be reloaded during the diagnostic, as determined by the gateway, no reload occurs and calls remain operational.

CAUTION
Loss of service
Call processing is dropped during a circuit controller reload.

GLC Card View shows the 4 lines circuits associated with a circuit controller by alternating the line circuit graphic color from dark blue to light blue. The following figure shows the GLC Card View and the allocation of circuits to circuit controllers.

GLC Card View showing allocation of circuits to circuit controllers



Card Attributes

CLEI Code: NotARealAB

Card Description: Nortel MG9k Global Line Card 32

Hardware Version: none 200

Firmware Version: 01 F

Software Version: 0

Serial Number: M64428V10

Manufacturer: Nortel Networks

PEC Code: NY53AB

Status

Availability Status: Normal

Usage Status: Idle

Standby Status: Providing_Service

Card Alarm Status: None

Procedural Status: Normal

Control Status:

State

Administrative State: Unlocked

Configuration State: Online

Operational State: Disabled

Critical: 0 Minor: 0

Major: 0 Warning: 0

You access the GLC Circuit Controller Diagnostic from the Line Circuit Diagnostic subsystem. GLC Circuit Controller Diagnostic can perform diagnostics on the following cards:

- GLC 32 (NTNY53AA and NTNY53BA)
- GLC 12 (NTNY53CA)

You must have maintenance privileges to perform this procedure.

When to use this procedure

Use these procedures when 4 circuits belonging to a single circuit controller appear in the operational disabled state.

Prerequisites

There are no prerequisites for this procedure.

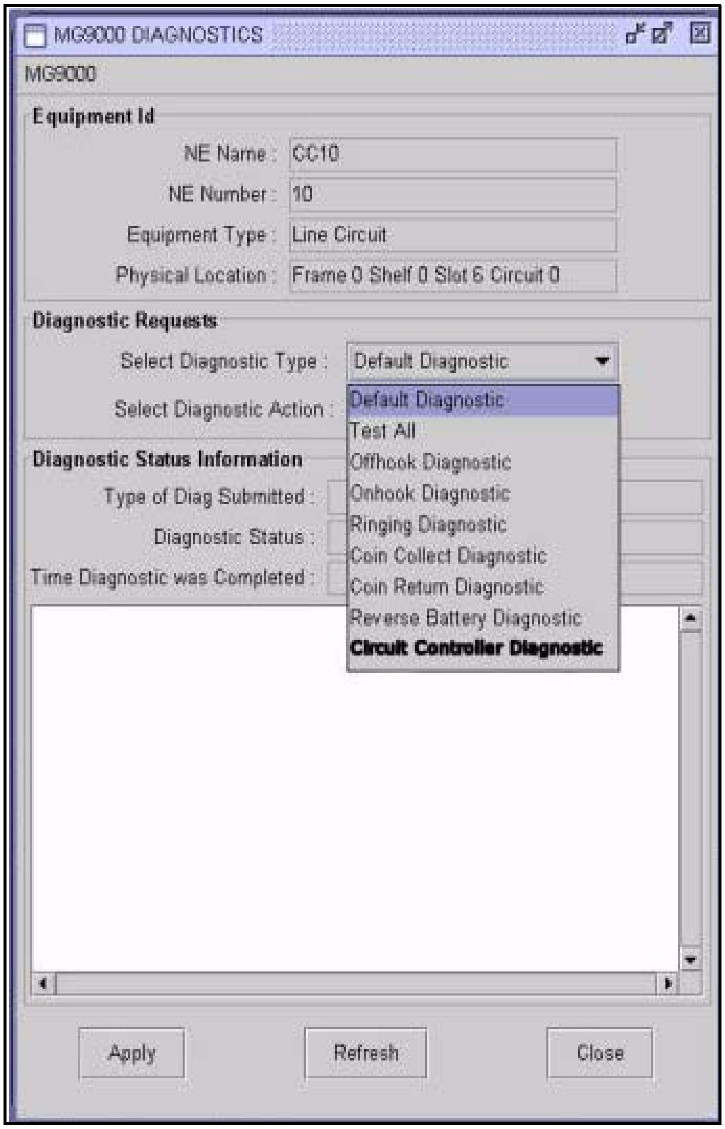
Action

Performing GLC circuit controller diagnostics

At the MG 9000 Manager

1. From the GLC Card View, select the Actions menu at the top of the screen. The Actions View screen appears.
2. Select Maintenance->Diagnostic. The Diagnostic View screen appears.
3. Select Circuit Controller Diagnostic in the Select Diagnostic Type field.

Diagnostic View



MG9000 DIAGNOSTICS

MG9000

Equipment Id

NE Name : CC10

NE Number : 10

Equipment Type : Line Circuit

Physical Location : Frame 0 Shelf 0 Slot 6 Circuit 0

Diagnostic Requests

Select Diagnostic Type : Default Diagnostic

Select Diagnostic Action :

Diagnostic Status Information

Type of Diag Submitted :

Diagnostic Status :

Time Diagnostic was Completed :

4 Select Perform Diagnostic in the Select Diagnostic Action field.

> ***Note:*** Normally this field is initially set to Perform Diagnostic. If the field is already set to Perform Diagnostic, go to step 5.

5 Click the Apply button at the bottom of the Diagnostic View. A dialog box appears indicating that the action will effect service on the 4 line circuits.

Click OK to continue, or Cancel to stop the procedure.

The system diagnoses each circuit controller. The gateway determines if a circuit controller needs to be reloaded. If a circuit controller does not need to be reloaded during the diagnostic, no reload occurs and calls remain operational.

6 This procedure is complete.

Aborting line circuits diagnostics

Purpose of this procedure

Use the following procedure to abort in-service or out-of-service diagnostics on line circuits connected to the following cards:

- World line card circuits (POTS 32 card)
- Global line card circuits (GLC 32 card)
- Service Adaptive Access circuits (SAA card) (not used in the UA-IP solution)
- Digital Subscriber Loop Voice and Data circuits (xDSL)

When to use this procedure

Use this procedure when it is necessary to Abort in-service or out-of-service line diagnostics.

Prerequisites

The MG 9000 must be executing line circuit diagnostics. Refer to Performing in-service line diagnostics or Performing out-of-service line diagnostics.

Action

Aborting in-service or out-of-service line diagnostics

At the MG 9000 Manager

1. At the Subnet View, double click the MG 9000 icon on which diagnostics are to be queried. The Frame View appears.
2. In the Frame View, double click on the shelf on which the circuits resides to be tested. The Shelf View appears.
3. In the Shelf View, double click on the World Line card (POTS 32), GLC 32 card, SAA card, or xDSL card on which the diagnostics are to be aborted.
4. In the left side of the Card View, double click on the circuit under test. The Circuit View screen appears.
5. From the Actions menu at the top of the screen, select Maintenance->Diagnostic. The MG 9000 Diagnostic View appears.
6. Determine if a Default Diagnostic or Destructive Diagnostic is in progress by performing the following steps:

- **a** Check to see if the Type of Diag Submitted field is set to Default Diagnostic.
- **b** Verify that the Diagnostic Status Field is set to InProgress.

7 Select the Abort Diagnostic in the Select Diagnostic Actions field.

8 Click the Apply button at the bottom of the Diagnostic View.

9 This procedure is complete.

DS1 IMA link pattern test

Purpose of this procedure

The DS1 IMA link pattern test is an in-service test for DS1-IMA links in a DS1-IMA group.

When to use this procedure

Use these procedures when it is necessary to perform IMA diagnostics.

Prerequisites

These procedures have no prerequisites.

Action

Performing DS1 IMA diagnostics

At the MG 9000 Manager

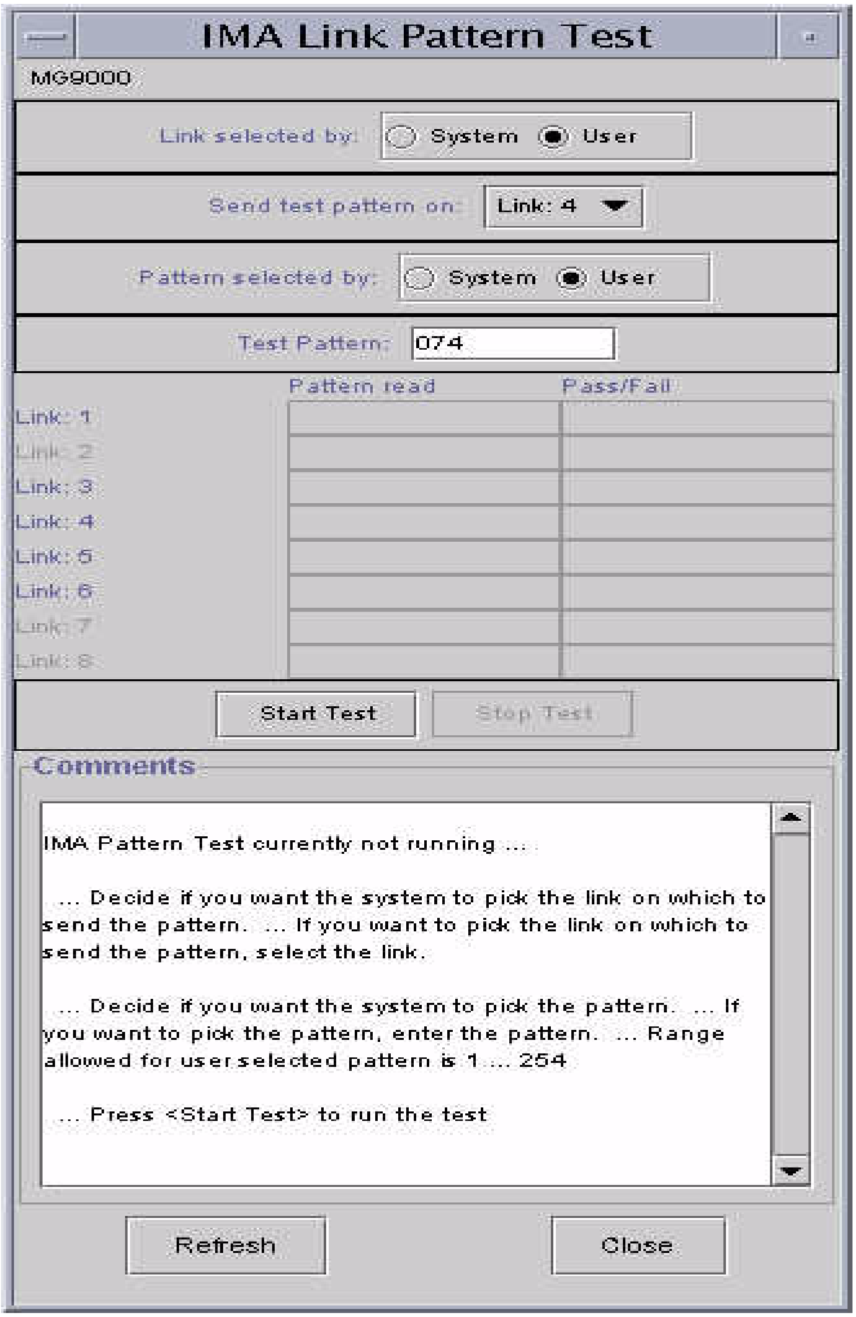
1 At the Subnet View, double click the MG 9000 icon on which diagnostics are to be run. The Frame View appears.

2 In the Frame View, double click on the shelf on which the circuits resides to be tested. The Shelf View appears.

3 In the Shelf View, double click on the active DS1 IMA card on which the diagnostics are to be run.

4 In the DS1 IMA Card View, from the menu bar at the top select Action->Maintenance->Pattern Test. The following IMA Link Pattern Test screen appears.

IMA Link Pattern Test View



Link selected by: ○ System ● User

Send test pattern on: Link: 4

Pattern selected by: ○ System ● User

Test Pattern: 074

	Pattern read	Pass/Fail
Link: 1		
Link: 2		
Link: 3		
Link: 4		
Link: 5		
Link: 6		
Link: 7		
Link: 8		

```
IMA Pattern Test currently not running ...

 ... Decide if you want the system to pick the link on which to
send the pattern.  ... If you want to pick the link on which to
send the pattern, select the link.

 ... Decide if you want the system to pick the pattern.  ... If
you want to pick the pattern, enter the pattern.  ... Range
allowed for user selected pattern is 1 ... 254

 ... Press <Start Test> to run the test
```

5 In the Link selected by panel, select User or System. Use the information in the following table to determine the next step.

If Link selected by is	Do
User	step 6
System	step 7

6 In the Send test pattern panel select a link number from the pick list.

7 In the Pattern selected by panel, select whether the test pattern is to be selected by the User or System. Use the information in the following table to determine the next step.

If Pattern selected by is	Do
User	step 8
System	step 9

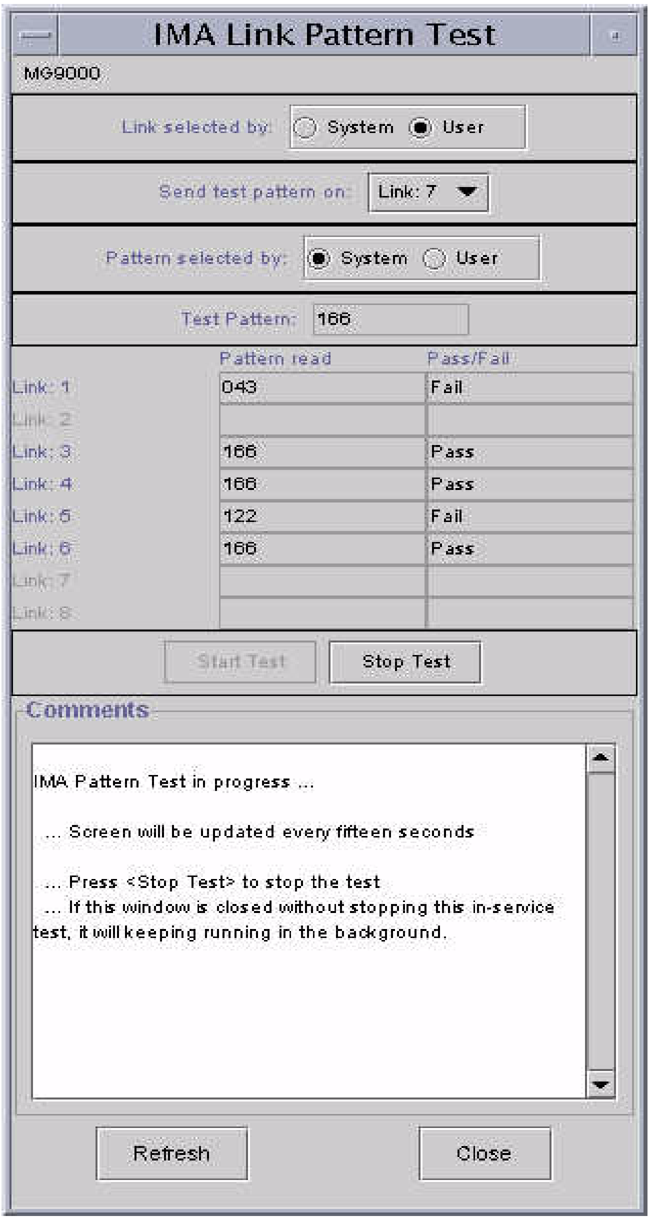
8 Enter a number from 1-254 in the Test Pattern panel representing the test pattern to be sent.

> ***Note:*** The number entered should match the number received after the test is run. If the number received does not match the number entered, the test is a failure.

9 Click on Start Test to run the test. The test results are displayed in the IMA Link Pattern Test View Comments pane.

The following figure shows the IMA ink Pattern Test View with the system reporting the test progress.

IMA Link Pattern Test View showing test progress



Link selected by: ○ System ● User

Send test pattern on: Link: 7

Pattern selected by: ● System ○ User

Test Pattern: 166

	Pattern read	Pass/Fail
Link: 1	043	Fail
Link: 2		
Link: 3	166	Pass
Link: 4	166	Pass
Link: 5	122	Fail
Link: 6	166	Pass
Link: 7		
Link: 8		

IMA Pattern Test in progress ...

... Screen will be updated every fifteen seconds

... Press <Stop Test> to stop the test
... If this window is closed without stopping this in-service test, it will keeping running in the background.

10 This procedure is complete.

DS1 IMA carrier test

Purpose of this procedure

The DS1 IMA carrier test is an out-of-service test for DS1 IMA ports. The test provides the user with the local loop-back and far-end loop-back configuration for all carriers. The user can set both tests with restrictions on some state transitions. An AIS test pattern can also be sent. A message box appears with the expected result for the successful completion of the test.

Note: The port to be tested must be locked prior to initiating the test.

When to use this procedure

Use these procedures when it is necessary to test out-of-service DS1 carriers.

Prerequisites

A pair of DS1 IMA cards must be installed in the data control cards (DCC) slots 10 and 11 of the master shelf.

Action

Performing a DS1 carrier test

At the MG 9000 Manager

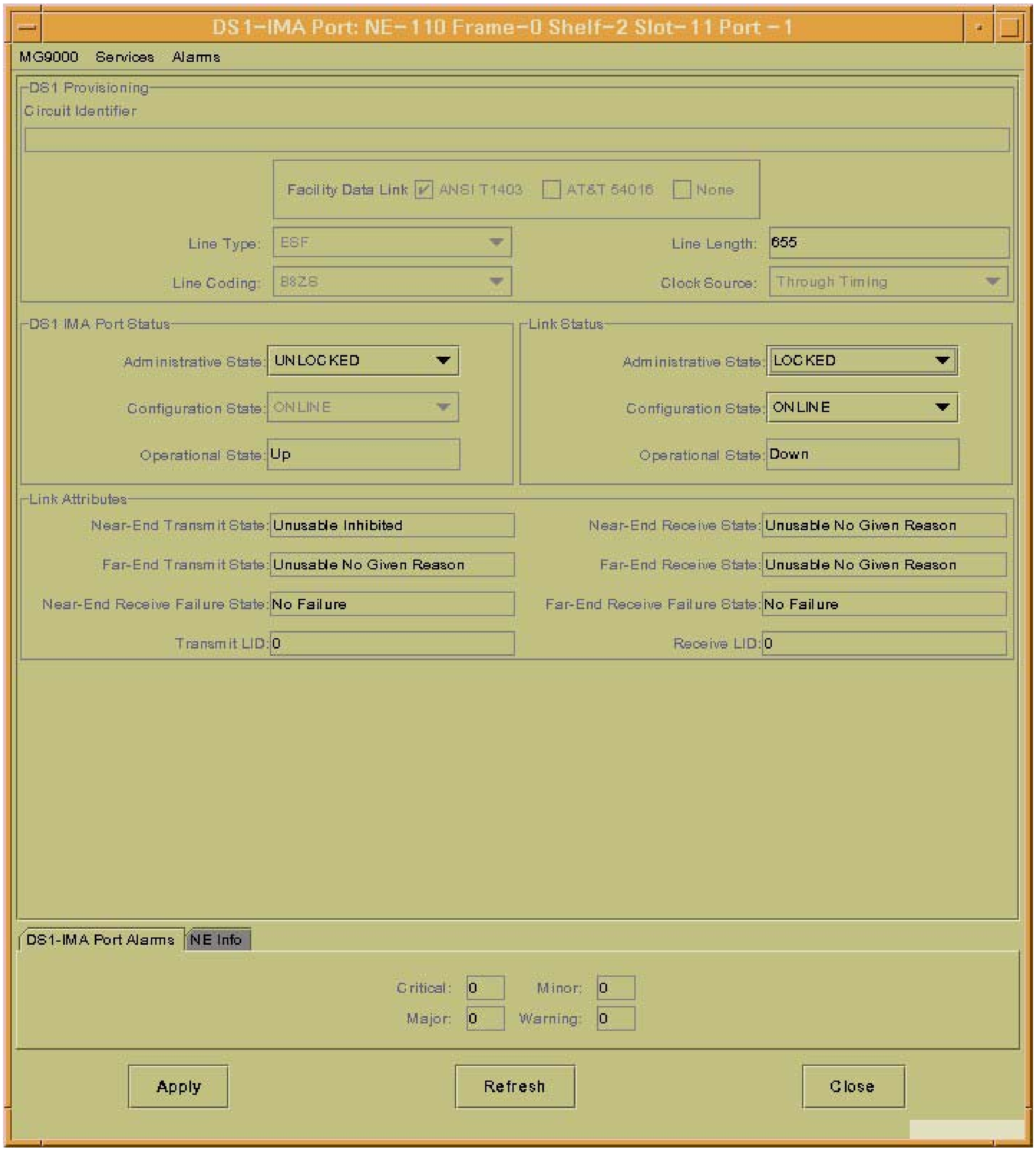
1 At the Subnet View, double click the MG 9000 icon on which diagnostics are to be run. The Frame View appears.

2 In the Frame View, double click on the shelf on which the circuits resides to be tested. The Shelf View appears.

3 In the Shelf View, double click on the active DS1 IMA card on which the diagnostics are to be run.

4 In the DS1 IMA Card View, click on the DS1-IMA port to be tested. The DS1-IMA Port View appears.

DS1-IMA Port View



DS1-IMA Port: NE-110 Frame-0 Shelf-2 Slot-11 Port -1

DS1 Provisioning

Circuit Identifier:

Facility Data Link ☑ ANSI T1403 □ AT&T 54016 □ None

Line Type: ESF

Line Length: 655

Line Coding: B8ZS

Clock Source: Through Timing

DS1 IMA Port Status

Administrative State: UNLOCKED

Configuration State: ONLINE

Operational State: Up

Link Status

Administrative State: LOCKED

Configuration State: ONLINE

Operational State: Down

Link Attributes

Near-End Transmit State:	Unusable Inhibited	Near-End Receive State:	Unusable No Given Reason
Far-End Transmit State:	Unusable No Given Reason	Far-End Receive State:	Unusable No Given Reason
Near-End Receive Failure State:	No Failure	Far-End Receive Failure State:	No Failure
Transmit LID:	0	Receive LID:	0

Critical:	0	Minor:	0
Major:	0	Warning:	0

5 At the DS1-IMA Port View, in the Link Status pane, set the Administrative State to Locked.

6 To remove the link from the IMA group, set the Configuration State to Offline.

7 In the DS1-IMA Port Status pane, set the Administrative State to Locked.

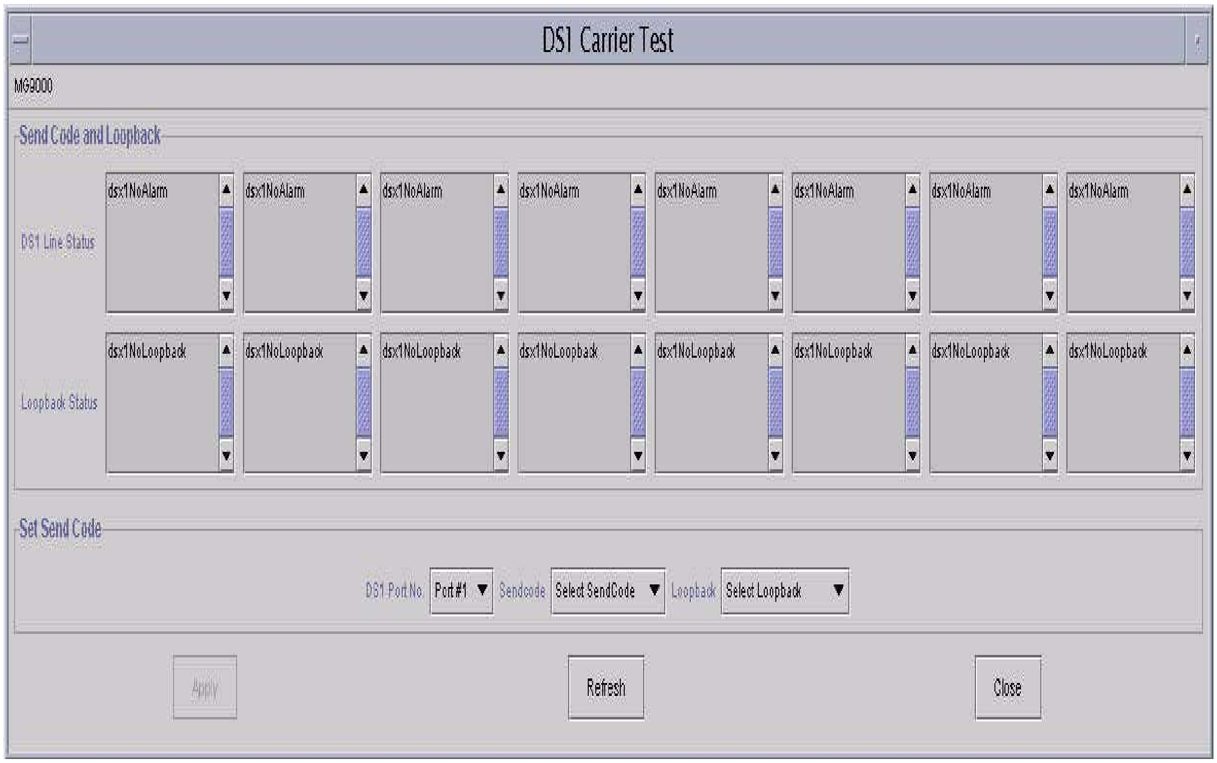
8 At the Shelf View, select Actions->Edit IMA Group from the menu bar. The Add/Remove Links to/from IMG Group View appears.

9 Select the links to be removed from the IMA Group by clicking in the box next to each link number, removing the check mark from the box. The DS1 link must be removed from the IMA Group before testing.

10 At the IMA Group View, click on Apply to submit the changes.

11 In the DS1 IMA Card View, from the menu bar select Action->Maintenance->Carrier Test. The DS1 Carrier Test View appears.

DS1 Carrier Test View



DS1 Carrier Test

MG9000

Send Code and Loopback

DS1 Line Status: dsx1NoAlarm | dsx1NoAlarm | dsx1NoAlarm | dsx1NoAlarm | dsx1NoAlarm | dsx1NoAlarm | dsx1NoAlarm | dsx1NoAlarm

Loopback Status: dsx1NoLoopback | dsx1NoLoopback | dsx1NoLoopback | dsx1NoLoopback | dsx1NoLoopback | dsx1NoLoopback | dsx1NoLoopback | dsx1NoLoopback

Set Send Code

DS1 Port No. Port#1 ▼ Sendcode Select SendCode ▼ Loopback Select Loopback ▼

12 In the Set Send Code pane, select the DS1 Port No. to be tested, the Send Code and Loopback options.

Use the following table to determine the selections in the Set Send Code pane.

DS1 Carrier Test View Send Code options

Set Send Code pane option	Option	Description
Send Code	Stop Tx AIS	Stop transmitting AIS signal on this interface towards the far end.
	Send Tx AIS	Transmit an AIS signal on this interface toward the far end.
Loopback	No loopback	No local loopbacks are configured on this interface. If a loopback has already been set, this option can be used to remove the setting.
	Line	The received signal at this interface does not go through the terminal device but is looped back out towards the far end.
	Payload	The received signal at this interface is looped through the terminal device and back out towards the far end.
	Terminal	The transmitted signal at this interface is looped back and received on the same interface.
	Dual (Line and Terminal)	Both Line and Terminal loopback are active simultaneously.

13 Click Apply to start the test.

14 To end the test, reset the Loopback and Sendcode fields.

15 If it is desired to re-add the tested link back into the IMA group, refer to procedure “Modifying (adding or deleting) links in the DS1 IMA group” in *MG 9000 Configuration Management*, NN10096-511.

16 This procedure is complete.

Testing lines

Purpose of this procedure

This section provides information on support for line testing.

The Services menu contains the following test parameter options:

- MTAP Test Manager used to support external test equipment for testing lines
- DTA Test Manager used to test private lines circuits

When to use this procedure

These procedures are used when it is necessary to test lines connected to the MG 9000.

Prerequisites

This procedure has no prerequisites.

Action

MTAP Test Manager

The metallic test access point (MTAP) line test screen provides an interface to pass line test commands from the MG 9000 Manager to external test equipment.

The Nortel Networks Access Care external test system has direct access to test heads collocated with the MG 9000 for line testing and communicates with the MG 9000 Manager and line test manager (LTM) through an ethernet port. The MG 9000 Manager software provides the line test management application to convert the Access Care parameters into commands that can be forwarded and processed in the MG 9000. The GUI specifies the test heads for Access Care use when testing a specified line circuit.

Using Access Care, a connection for metallic test access (MTA) to a line card can be set up by entering a directory number (DN). Once the test connection is established, the test direction can be changed from “normal” (looking out) to “looking in” or “bridged.”

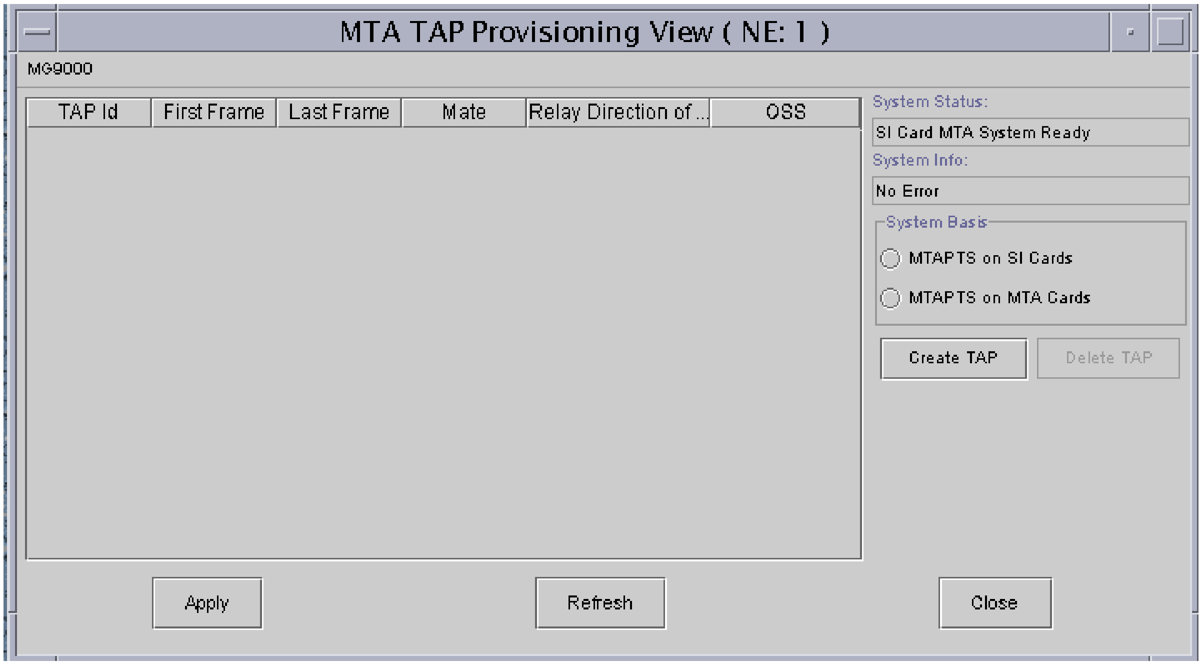
> ***Note:*** With “bridged” connections, the connection is often dropped while taking measurements with the Tollgrade DMU test head. A short current spike used for measurement purposes is sufficient to cause the line card to go into hazard protection mode, which in turn drops the connection. To perform another test, a new test connection must be established.

If the measurement is being taken to check talk battery voltage, use the “looking in” direction. The “normal” direction (looking out) is sufficient for troubleshooting loop problems.

The potential exists for this behavior using other direct-connect test heads and NTT-based test heads, however, no other scenarios have been tested.

The following figure shows the MTA TAP Provisioning View screen.

MTA TAP Provisioning View Screen



MTA TAP Provisioning View (NE: 1)

MG9000

TAP Id	First Frame	Last Frame	Mate	Relay Direction of ...	OSS

System Status: SI Card MTA System Ready

System Info: No Error

System Basis

○ MTAPTS on SI Cards

○ MTAPTS on MTA Cards

MTA TAP Provisioning View fields

Field	Explanation
TAP Id	The test access point (TAP).
FirstFrame	The first frame which indicates the beginning of the range of frames for a particular TAP.
LastFrame	The last frame which indicates the end of the range of frames for a particular TAP.
Mate	If the TAP can be used to make up a 4-wire pair, this field contains the mate TAP.

MTA TAP Provisioning View fields

Field	Explanation
Relay Direction of	Used for full-split connections, indicates the hard-wired direction for the TAP (TestIn, TestOut). This field only pertains to mated TAP pairs.
OSS	Indicates the origin of the provisioned TAP. The options are AccessCare or CS2000 Manager GUI.
System Status	Provides current hardware (SIC or MTA card) status.
System Info	Provides hardware information.
System Basis	Two radio buttons are provided that allow the user to select the basis for line testing based on hardware availability (SIC or MTA card).

Note: When switching from one existing configuration to another, if any MTAPTs are provisioned, all the old MTAPTs on that MG 9000 must be deleted first.

Setting up the MTAP Test Manager

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon on which an MTAP Test Manager is to be set up. The Frame View appears.

2 In the Frame View, double click on the master shelf. The Shelf View appears.

3 From the Services menu at the top of the Shelf or Card View, select MTAP Test Manager. The MTA Provisioning View appears.

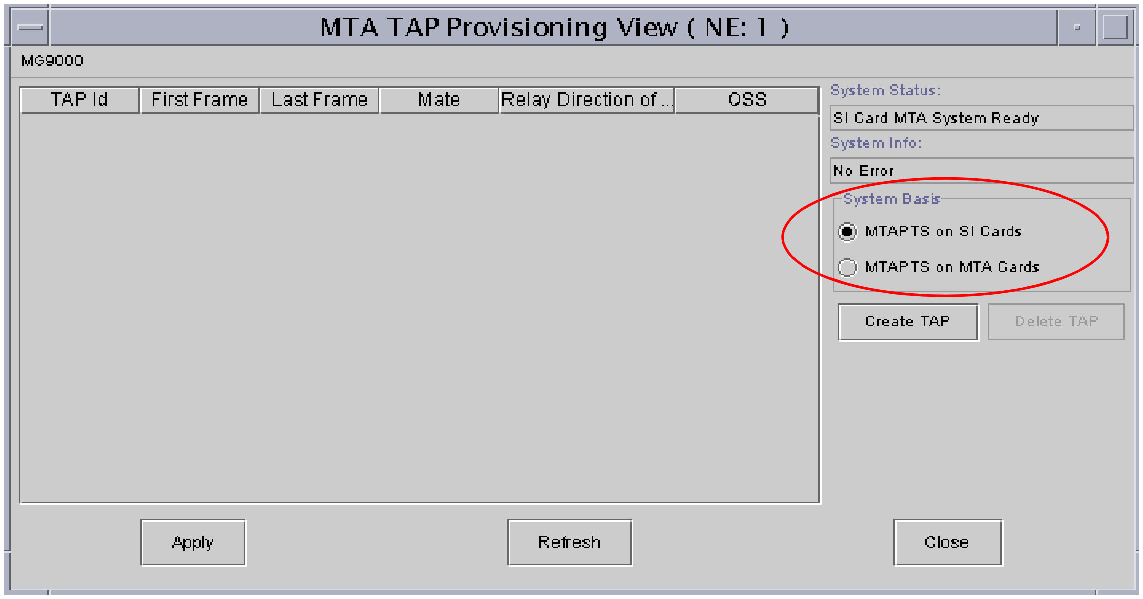
4 Set the System Basis by selecting the radio button that represents the card on which to set the MTAPTS, whether on an SI or MTA card. The following figure shows the MTA TAP Provisioning View with the System Basis area highlighted.

Note 1: The System Status reports MTA Card MTA System Ready when an MTA card is installed, whether the SI Card or the MTA card is used. If no MTA card is provisioned, the System Status is reported as SI Card MTA System Ready.

Note 2: If no selection is made, the system responds with an error message informing that no System Basis selection was made.

Note 3: The MTAPTS on MTA cards can be selected as the System Basis only if the hardware can support the MTA card configuration, meaning an MTA card is provisioned in the MG 9000. If an attempt is made to select MTAPTS on MTA cards and no MTA card is provisioned in the MG 9000, the system responds with a No Support error informing the user that the system does not support MTA card configuration.

MTA TAP Provisioning View



System Status: SI Card MTA System Ready

System Info: No Error

System Basis

● MTAPTS on SI Cards

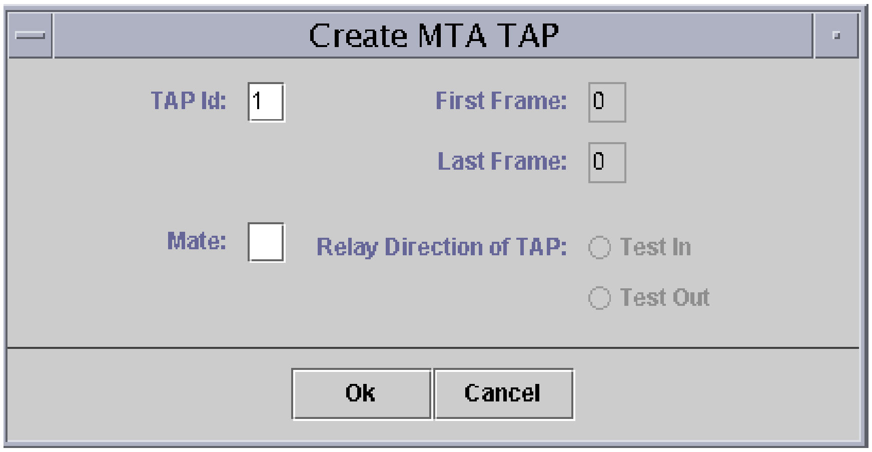
○ MTAPTS on MTA Cards

5 The next step depends on the information in the following table.

If you selected	Do
MTAPTS on SI Cards	step 6
MTAPTS on MTA Cards	step 8

6 Click on the “Create TAP” button to create a test access point.

Create MTA TAP View for MTAPTS on SI Cards



Create MTA TAP

TAP Id: 1

First Frame: 0

Last Frame: 0

Mate:

Relay Direction of TAP: ○ Test In ○ Test Out

The “Relay direction” field applies only to a “Mate” TAP. Some MTA tests require a full-split connection, which is composed of two TAPs. One TAP is connected to ‘Test In’, while the other TAP is connected to ‘Test Out’. The ‘Relay Direction’ can only be set with the ‘Mate’ field filled in.

The “Delete TAP” button removes a highlighted TAP from the MTA TAP View screen and deprovisions that TAP from the MG 9000

7 A SIC card configuration requires frames to be wired together in pairs. Each pair of frames has 4 TAPs, so up to 4 test heads can be connected. If there is an odd number of frames in the configuration, the last frame contains a full set of 4 TAPs. The MTAP numbering is always from left to right. The following table shows the MTAP numbering scheme.

SIC MTAP/Frame Numbering Scheme

MTAP	Service Frame
1 through 4	1 and 2
5 through 8	3 and 4
9 through 12	5 and 6
13 through 16	7 and 8

The following table lists the valid mate settings for a SIC configuration.

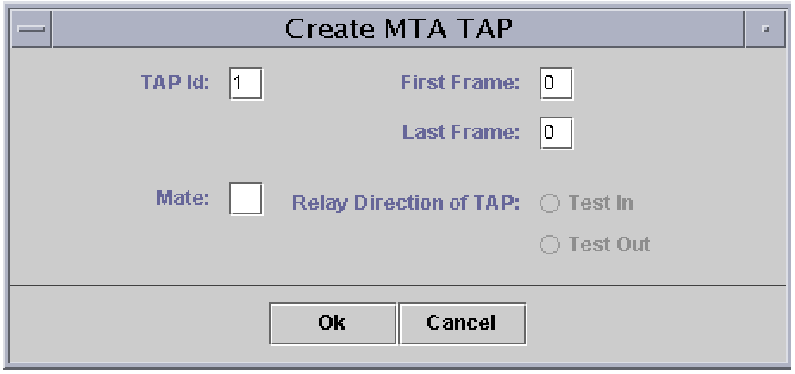
Valid Mates for SIC Configuration

MTAP	Valid Mates	MTAP	Valid Mates
1	2, 3, or 4	9	10, 11, or 12
2	1, 3, or 4	10	9, 11, or 12
3	1, 2, or 4	11	9, 10, or 12
4	1, 2, or 3	12	9, 10, or 11
5	6, 7, or 8	13	14, 15, or 16
6	5, 7, or 8	14	13, 15, or 16
7	5, 6, or 8	15	13, 14, or 16
8	5, 6, or 7	16	13, 14, or 15

Go to step 12.

8 Click Create TAP. The Create MTA TAP View appears.

Create MTA TAP View for MTAPTS on MTA card



Create MTA TAP

TAP Id: 1

First Frame: 0

Last Frame: 0

Mate:

Relay Direction of TAP: ○ Test In ○ Test Out

9 Enter valid data in the First Frame and Last Frame fields.

10 Enter valid Mate TAP. The highest possible MTAPT is 8. The possible mate is from 1 to 8, except itself. Click OK.

11 Respond to the No Test Direction message that appears. Select the Test Direction.

12 This procedure is complete.

Deleting a TAP

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon on which an MTAP Test Manager is to be set up. The Frame View appears.

2 In the Frame View, select Services->MTAP Test Manager from the menu bar to access the MTA Provisioning View. the MTA Provisioning View appears.

> ***Note:*** The MTA Provisioning View can also be accessed from the Shelf View or Card View by selecting Services->MTAP Test Manager from the menu bar at the top of the Shelf or Card View.

3 Select the TAP to be deleted.

4 Click Delete. Respond to the verification message to delete the TAP.

5 This procedure is complete.

DTA Test Manager

DTA (Digital Test Access) is the functionality utilized to test private lines circuits (both DS1 and DS0 bundles) by setting up test access connections with external test equipment. Compatible external test systems pass TL1 (Transaction Language 1) requests through an Ethernet port to the MG 9000 Manager to setup appropriate MG 9000 connections to collocated testheads or remote test units (RTU). The following table lists the Ethernet port used for TL1 requests in the MG 9000 Manager based on software release.

Ethernet port usage for TL1 requests for MG 9000 Manager

TL1 requests for MG 9000 Manager in software release	Ethernet port number
SN05	2361
SN06	2362
SN06.2	2366
SN07, SN08	2363

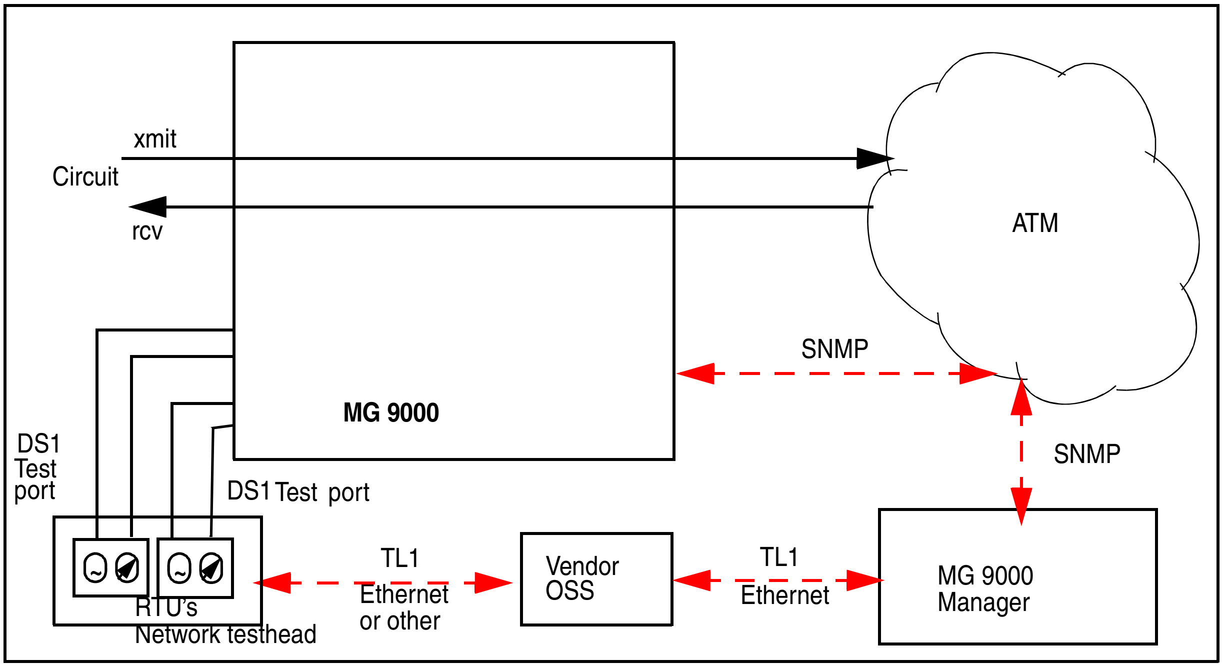
The DTA Test Manager screen is used to provision test access ports (TAP’s) in the MG 9000 which identify RTU’s that are specified in the external test system. Both monitor and split access of private line circuits is supported through DS1 DFAD (Dual Facilities Access Digroup) and DS1 TAD (Test Access Digroup) TAP's.

Digital test access on the MG 9000 consists of the following steps:

1. Provision DS1 ports as DFADs or TADs to be used for test access. Procedures for provisioning DFADs and TADs follow.
2. Provide digital test access by performing the following:
   - Use the vendor's test operations support system (OSS) to request/change test access to a particular circuit. Access a circuit in MONEF mode (non-intrusively) before changing the access mode to SPLTEF (intrusively). It is permissible to change from SPLTEF to MONEF. Once access is gained, the vendor's OSS and the testhead control the testing of the circuit.
   - Remove test access to the circuit to return the circuit to its pre-test access state.

The following figure shows the MG 9000 digital test access using an RTU.

MG 9000 DTA testing



Provisioning DFADs and TADs

To provide connectivity between the RTU and the MG 9000, DS1 ports on the MG 9000 must be defined as DFADs and/or TADs, and those ports must be connected to the associated ports on the RTU. Provisioning of the DFADs and TADs occur at the SNM.

Test access ports/paths (TAP) are test interface connections on a network element such as a digital cross connect system (DCS) that connect to a TSC or RTU testhead facility access digroup (FAD) or test access digroup (TAD). They are used to provide monitor or split test access for digital circuits that are provisioned on the NE. A TAP is a logical representation of the test connection required to test the proposed facility. When testing a DS0 service the TAP would represent 2 adjacent channels within the DS1 TAD. When testing a DS1 service the TAP would represent a single DS1 facility known as a FAD.

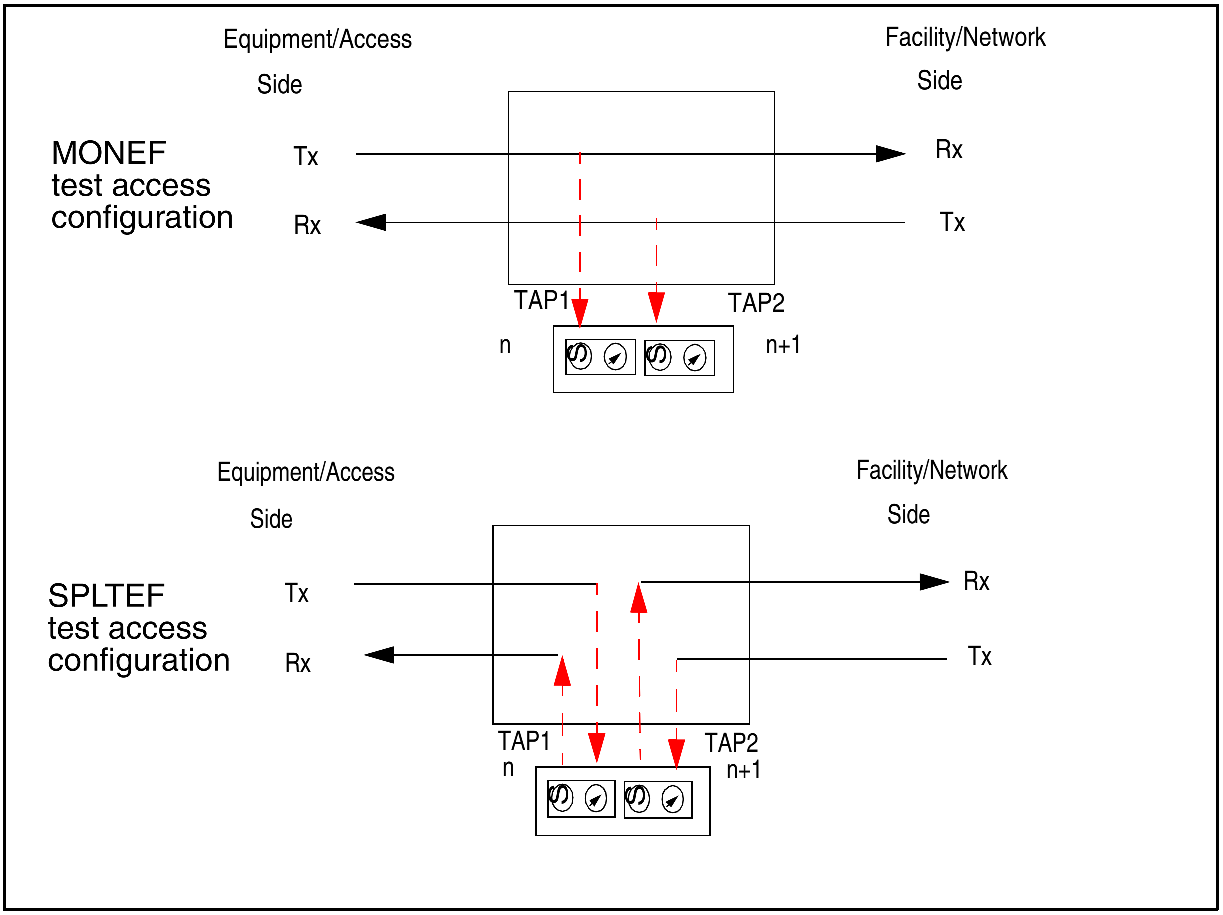
DFAD When provisioning a TAP, the MG 9000 Manager allows the technician to provision a DFAD or a TAD. When provisioning a DFAD, two DS1 ports are required. The first TAP provisioned will be used for the equipment side of the test connection, and must have an odd numbered TAP. A second TAP is always paired with the odd numbered (odd-numbered TAP + 1) since DFAD requires 2 TAPs. The second TAP is used for the facility side of the connection. Next, the MG 9000 Manager notifies the MG 9000 of the provisioning request. The MG 9000 Manager reserves the ports for DTA so that they cannot carry private line traffic.

In a DFAD configuration, TAPs are paired such that both the equipment and facility sides of the connection can be monitored or split simultaneously. DFAD supports testing of DS1s and DS0 bundles. DFAD employs the following two access modes.

- MONEF - provides hitless monitor access to both the transmit and receive paths of a circuit simultaneously and non-intrusively
- SPLTEF - provides simultaneous split access to both the equipment and facility sides of the circuit. Split access gives control of the transmit and receive paths to the test equipment. External test equipment tests in one direction and provides a keep-alive signal in the non-test direction. This is a service-affecting test access mode, but only affects the scope of the service that is, DS0 bundle test access only affects the DS0 bundle under test and is hitless on the DS1 and other DS0 bundle circuits carried on the DS1).

The following figure shows the two DFAD test access modes

DFAD MONEF and SPLTEF test access modes



The following procedure provides the steps for setting up a DFAD at the MG 9000 Manager. A prerequisite to performing this procedure is that the MG 9000 Manager TL1 software must be running to bring up the TL1 port. Any DS1 can be used as a TAP.

Provisioning a DFAD

At the MG 9000 Manager

1 Access the DS1 View screen.

2 Double click on a port number, for example, 15.

3 Set the following values in the DS1 View screen, and then click the Apply button.

- Line type = unframed
- Line coding = B8ZS
- Facility Data Link = None

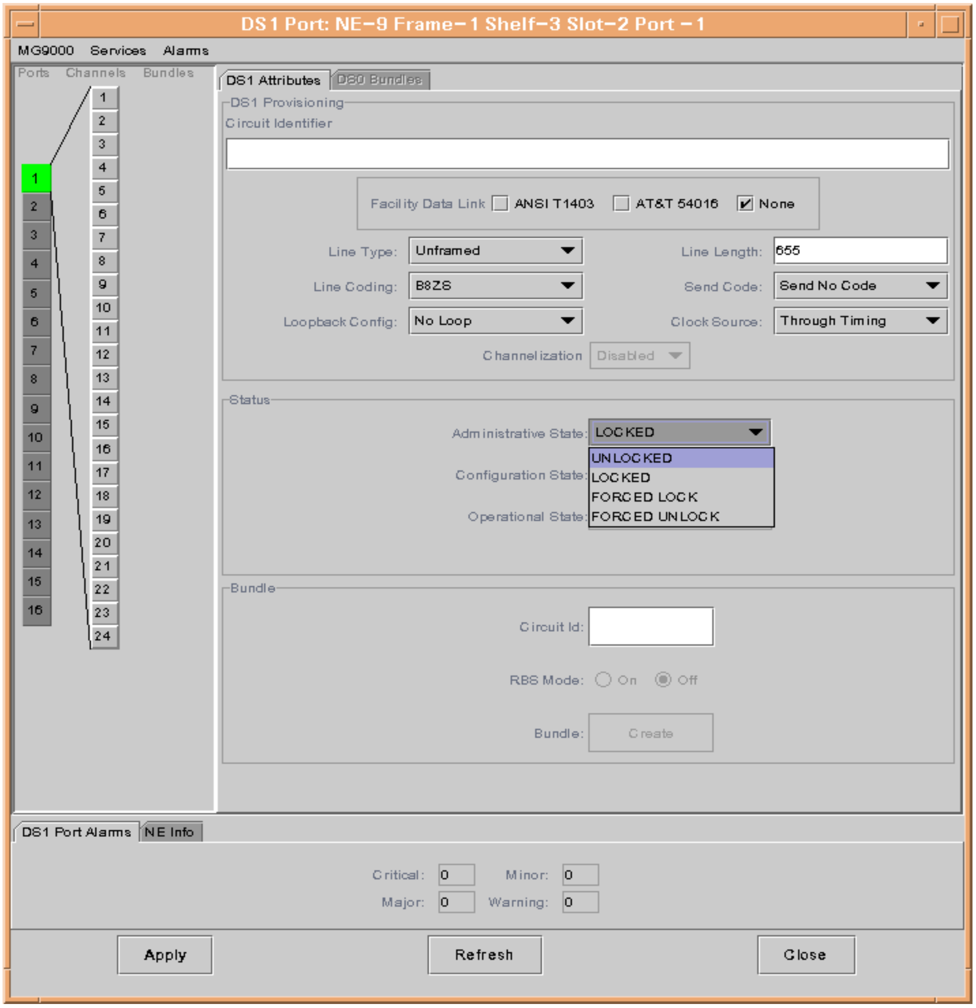
4 Determine if the DS1 has been wired to the test head.

If	Do
the DS1 port is already wired to the test head through the local wiring panel, such as a DSX panel	Step 5
the DS1 port is not wired to the test head	Go to the local wiring panel (such as DSX panel) according to local procedures and wire the DS1 to the test head and return to this step.

5 Set the port to Online.

6 Unlock the port.

Unlocking the port



DS1 Port: NE-9 Frame-1 Shelf-3 Slot-2 Port -1

DS1 Provisioning

Circuit Identifier:

Facility Data Link □ ANSI T1403 □ AT&T 54016 ☑ None

Line Type: Unframed

Line Length: 655

Line Coding: B8ZS

Send Code: Send No Code

Loopback Config: No Loop

Clock Source: Through Timing

Channelization: Disabled

Status

Administrative State: LOCKED

Configuration State:

Operational State:

Bundle

Circuit Id:

RBS Mode: ○ On ● Off

Bundle: Create

Critical: 0 Minor: 0

Major: 0 Warning: 0

The Operational state becomes Enabled.

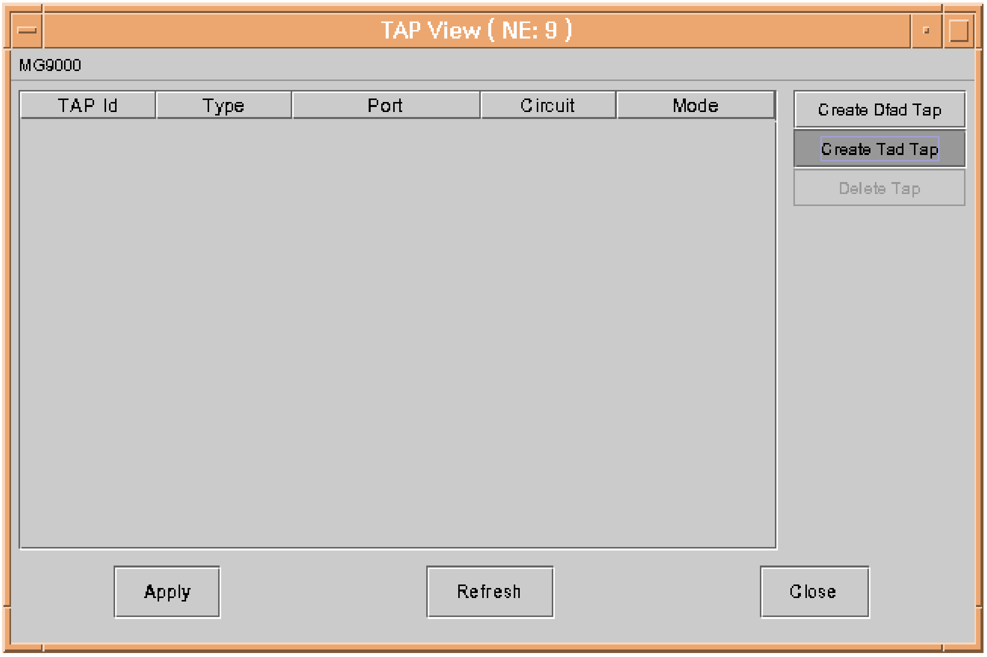
7 Select another port on the DS1 card or on another DS1 card in the shelf and repeat steps 1 through 6.

8 Go to the Services menu and select the pull down DTA Test Manager menu.

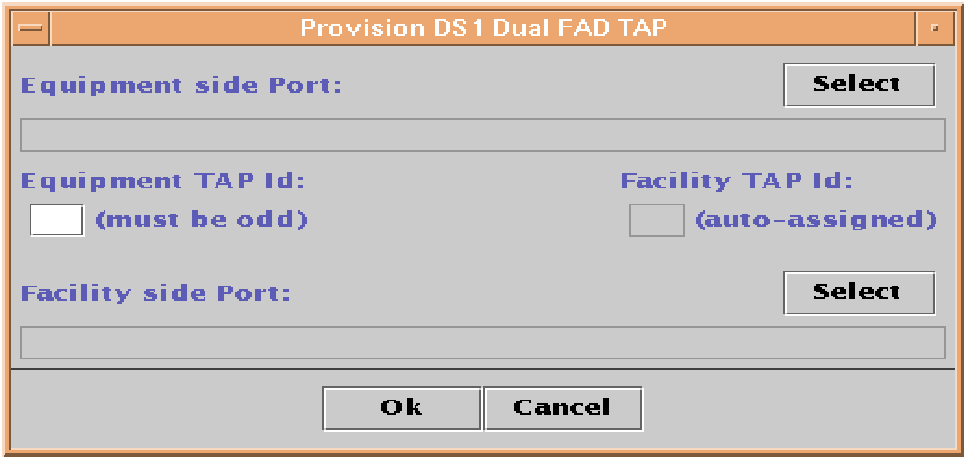
9 Select Create Dfad TAP.

A Provision DS1 Dual FAD TAP window appears.

TAP View window



Provision DS1 Dual FAD TAP window



10 Click on Equipment Side Port Select button and a NE Selector window appears. To select the card and port, click OK. At this point the card and port information will be entered in the empty field in the Provision DS1 Dual FAD TAP screen.

11 Select the facility side port by clicking on the Facility Side port select button.

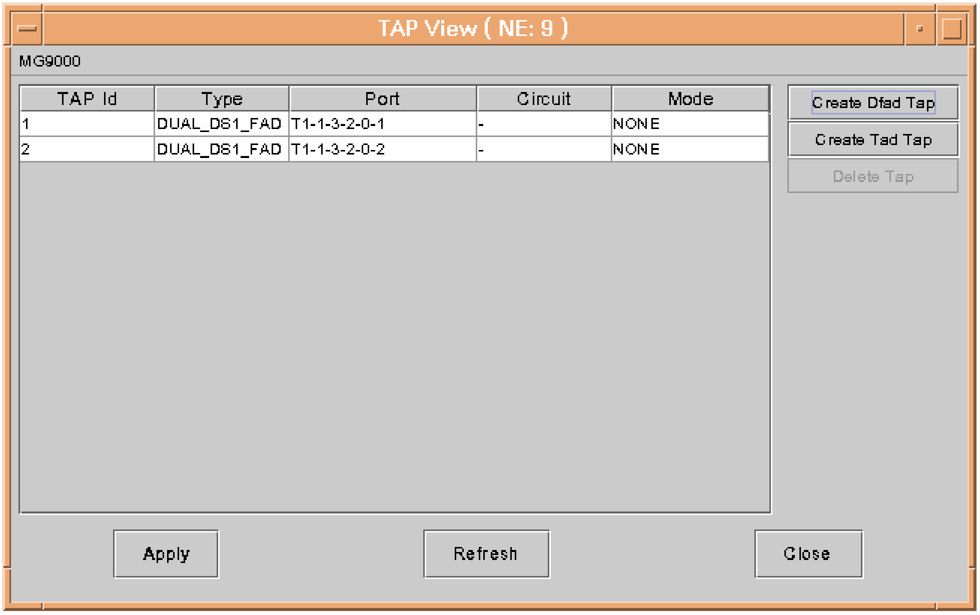
12 The NE Selector window appears. Select the Facility Side card and port by clicking OK. The port information appears in the Facility.

13 Select Equip TAP ID, based on the vendor requirements and local procedure.

14 Click OK.

15 The following window appears with the TAP information filled in.

TAP View with TAP data entered



TAP Id	Type	Port	Circuit	Mode
1	DUAL_DS1_FAD	T1-1-3-2-0-1	-	NONE
2	DUAL_DS1_FAD	T1-1-3-2-0-2	-	NONE

16 This procedure is complete.

The following procedure provides the steps for deleting a DFAD.

Deleting a DFAD

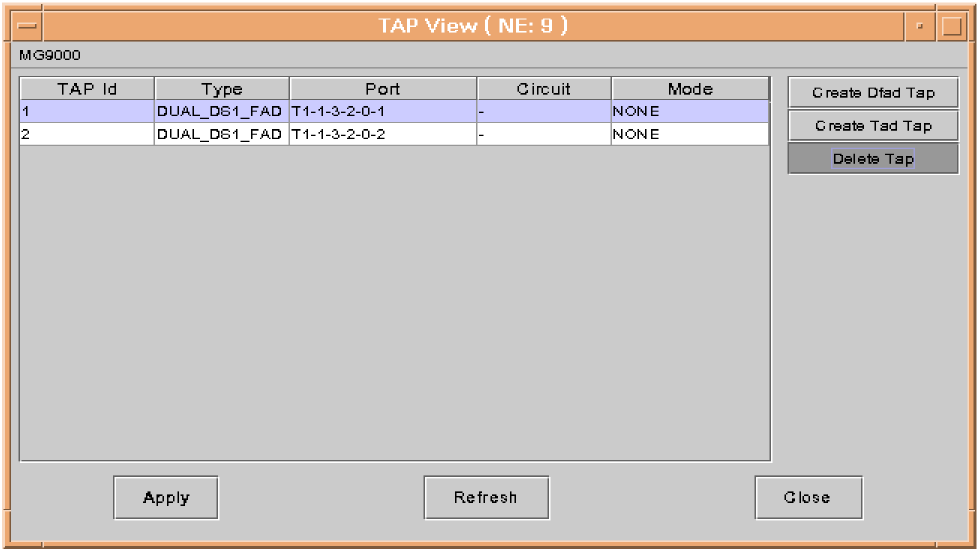
At the MG 9000 Manager

1 At the Shelf View, go to the Services menu and select DTA Test Manager.

2 At the TAP View, verify that there is currently no test access (MONEF or SPLTEF) on either TAP of the DFAD to be deleted. Select one row of the DFAD to be deleted. The DFAD entries are adjacent to one another.

3 Click Delete TAP. The TAPs are removed.

TAP View with Delete TAP selected



TAP View (NE: 9)

MG9000

TAP Id	Type	Port	Circuit	Mode
1	DUAL_DS1_FAD	T1-1-3-2-0-1	-	NONE
2	DUAL_DS1_FAD	T1-1-3-2-0-2	-	NONE

4 Click Close.

5 This procedure is complete.

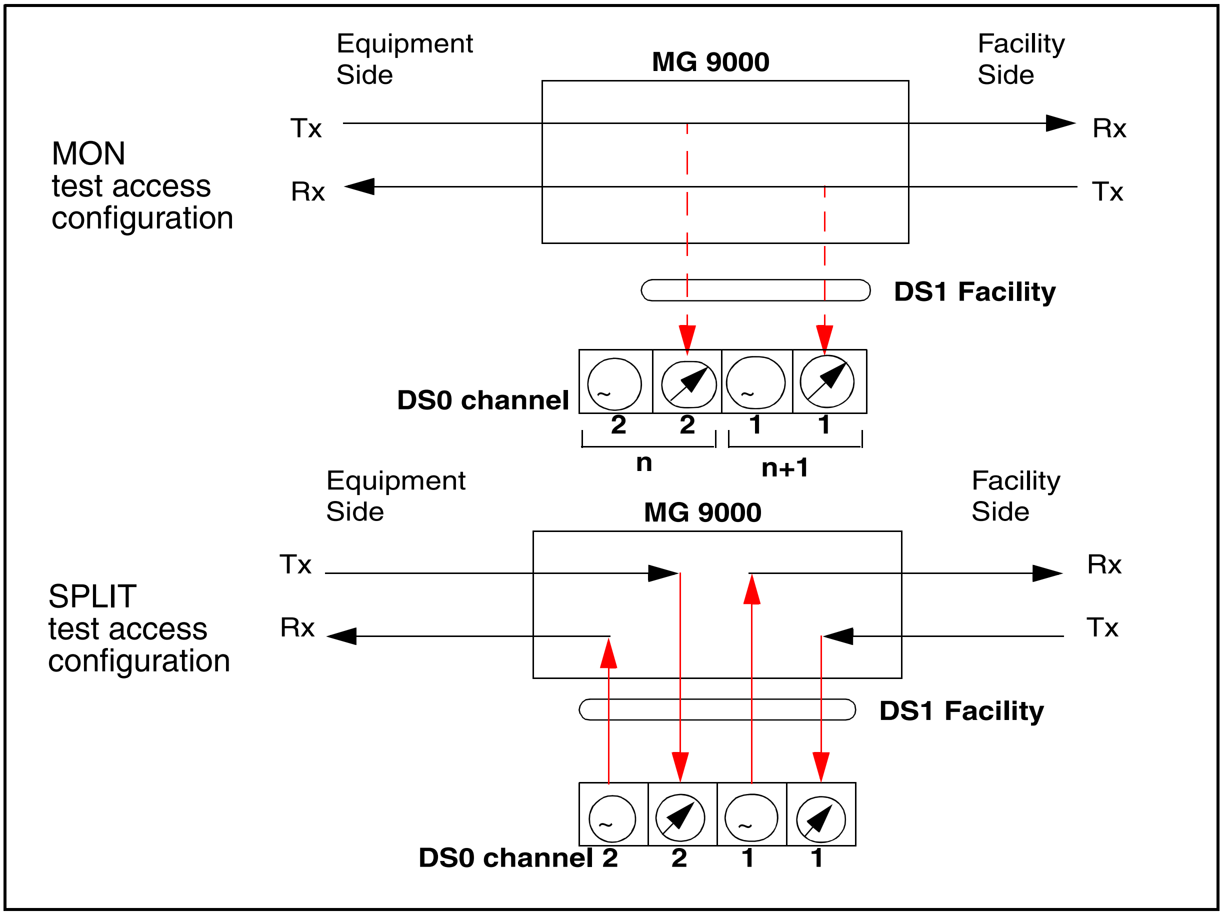
TAD When provisioning a TAD, twelve contiguous TAPs are automatically allocated over the DS1. Each TAP is associated with two adjacent channels within the DS1 TAD. The first TAP is associated with channel 1 and channel 2, the second TAP is associated with channel 3 and channel 4. This sequence continues until the twelfth TAP is associated to channel 23 and channel 24. The odd channel of the TAP is used for connections to the facility side of the circuit under test and the even channel number of the TAP is used for connections to the equipment side of the circuit. TAD test access only supports single channel DS0 bundles. TAD employs the following two test access modes.

- MONEF - The monitor connection of a single-channel DS0 bundle circuit utilizing a TAD is hitless on the circuit and all other circuits in the parent DS1. The receive direction of both the facility and equipment sides of the circuit under test are connected to the TAP and thus the test equipment.
- SPLTEF - The split connection onto the DS0 channel using a TAD connection is allowed only after a monitor connection is made.

When a change in access command is initiated the circuit under test is connected so that both the incoming and outgoing signal directions for the equipment and facility sides of the circuit are connected to the TAP. The access connection for the channel under test is intrusive but the channels not selected for access are not affected.

The following figure shows the two TAD test access modes

TAD MONEF and SPLTEF test access modes



The following procedure provides the steps for setting up a TAD at the MG 9000 Manager. A prerequisite to performing this procedure is that the CS2E TL1 software must be run to bring up the TL1 port. Any DS1 can be used as a TAP.

Provisioning a TAD

At the MG 9000 Manager

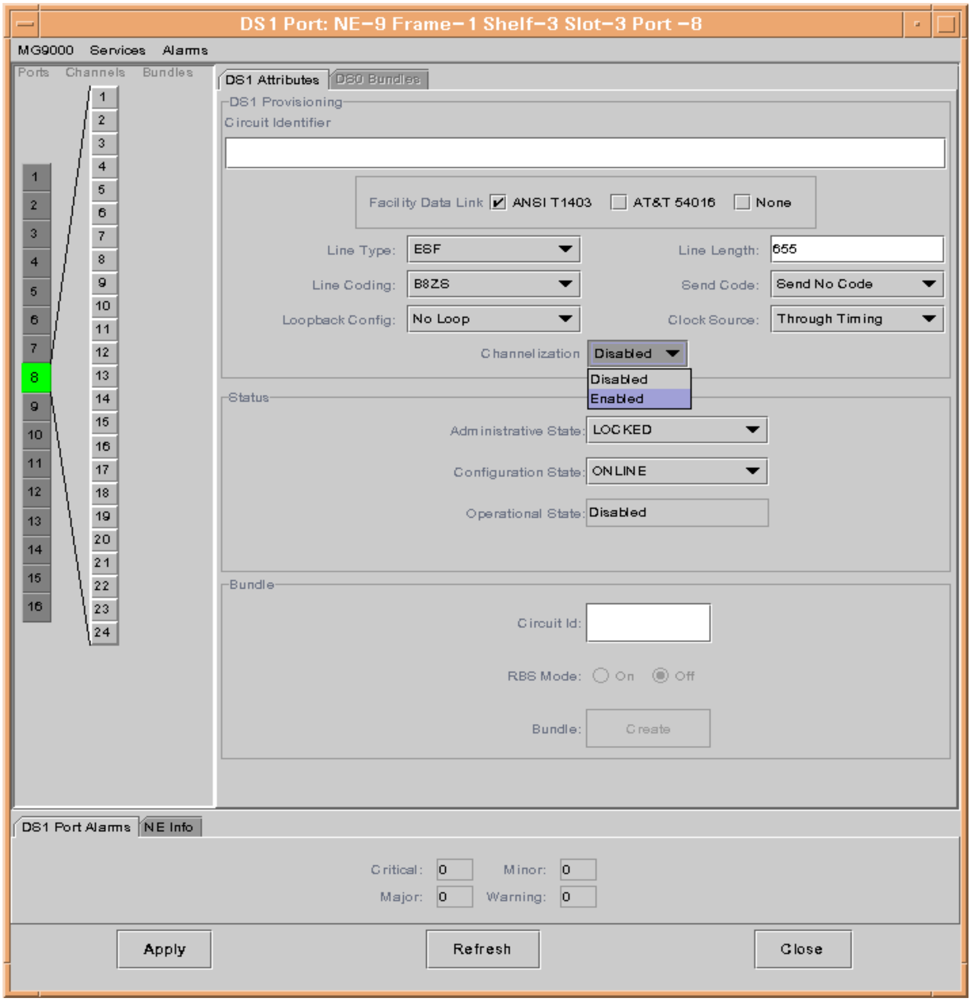
1 Access the DS1 View screen.

2 Double click on the desired port number, for example, 15. The Port View window appears.

3 Set the following values in the DS1 View screen

- Line type = ESF
- Line config = B8ZS
- Loopback = No loop
- Line length: enter the approximate length (in feet) of the DS1 to the test head
- Send code = Send no code
- Clock source = Through (default)
- Facility Data Line = None

DS1 Port View



DS1 Port: NE–9 Frame–1 Shelf–3 Slot–3 Port –8

DS1 Provisioning

Circuit Identifier:

Facility Data Link ☑ ANSI T1403 □ AT&T 54016 □ None

Line Type: ESF

Line Length: 655

Line Coding: B8ZS

Send Code: Send No Code

Loopback Config: No Loop

Clock Source: Through Timing

Channelization: Disabled

Status

Administrative State: LOCKED

Configuration State: ONLINE

Operational State: Disabled

Bundle

Circuit Id:

RBS Mode: ○ On ● Off

Bundle: Create

Critical: 0 Minor: 0

Major: 0 Warning: 0

4 Click on Apply.

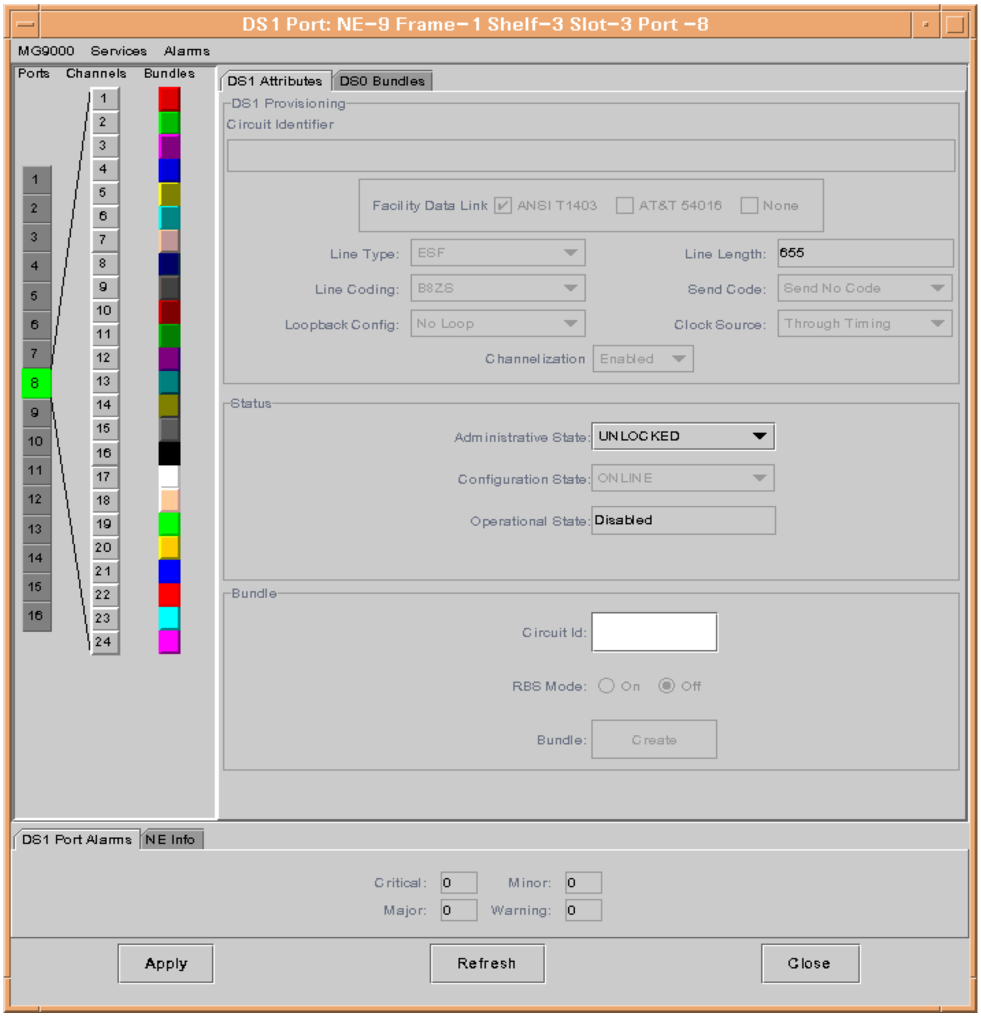
5 Determine if the DS1 has been wired to the test head.

If	Do
the DS1 port is already wired to the test head through the local wiring panel, such as a DSX panel	Step 6
the DS1 port is not wired to the test head	Go to the local wiring panel (such as DSX panel) according to local procedures and wire the DS1 to the test head and return to this step.

6 Set the port to On line.

7 In the DS1 View, set Channelization to Enabled. At this point the channels in the left side of the DS1 View will turn blue.

DS1 Port View with Channelization Enabled



DS1 Port: NE-9 Frame-1 Shelf-3 Slot-3 Port -8

DS1 Provisioning

Circuit Identifier

Facility Data Link ☑ ANSI T1403 □ AT&T 54016 □ None

Line Type: ESF

Line Length: 655

Line Coding: B8ZS

Send Code: Send No Code

Loopback Config: No Loop

Clock Source: Through Timing

Channelization Enabled

Status

Administrative State: UNLOCKED

Configuration State: ONLINE

Operational State: Disabled

Bundle

Circuit Id:

RBS Mode: ○ On ● Off

Bundle: Create

Critical: 0 Minor: 0

Major: 0 Warning: 0

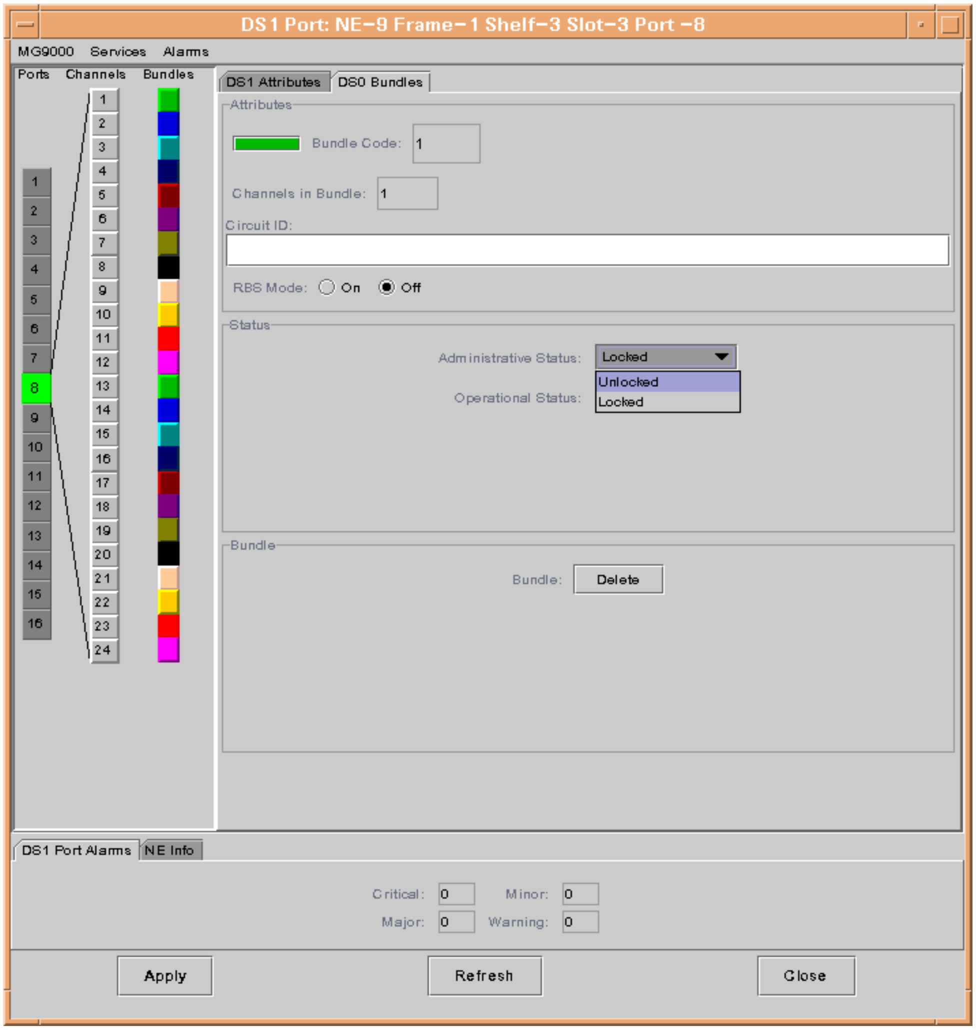
8 Unlock the port.

The Operational state becomes Enabled.

9 Click on each channel then click on Bundle Create. (Robbed bit signaling [RBS] default = Off.) Repeat this step for all 24 channels in order from 0 to 23.

10 Then unlock each bundle by double clicking and changing the Administrative state to Unlocked. Repeat this step for all 24 channels in order from 0 to 23.

DS1 Port View unlocking bundles



DS1 Port: NE−9 Frame−1 Shelf−3 Slot−3 Port −8

Bundle Code: 1

Channels in Bundle: 1

Circuit ID:

RBS Mode: ○ On ● Off

Administrative Status: Locked

Unlocked
Locked

Operational Status:

Bundle:

Critical: 0 Minor: 0

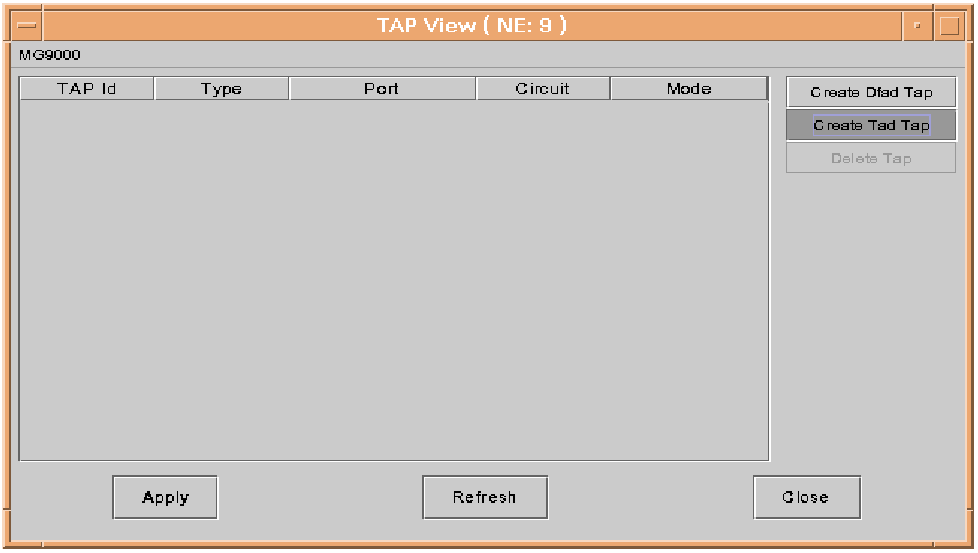
Major: 0 Warning: 0

11 At the Services menu, select DTA Test Manager. This brings up the TAP view.

12 Select Create TAD TAP.

A Provision DS0 TAD TAP window appears.

Creating a TAD TAP from the TAP View



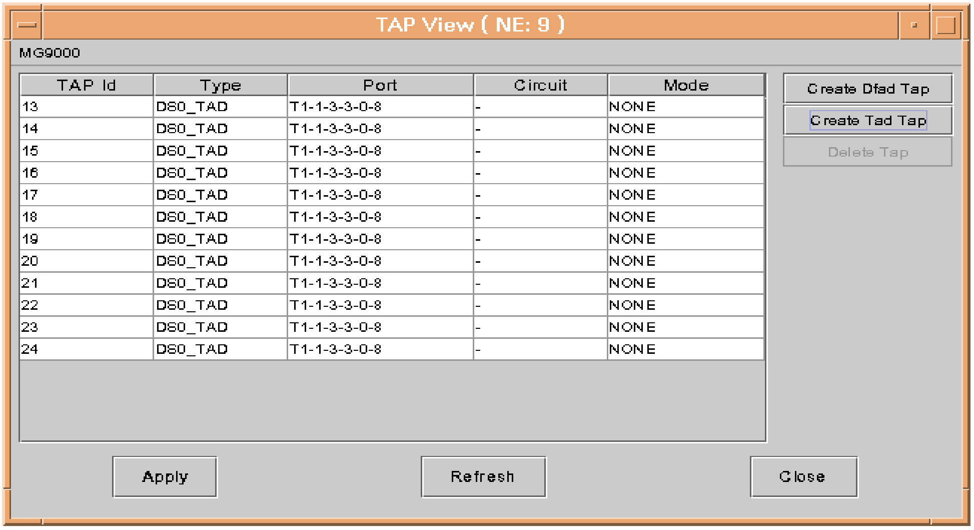
13 Click Select. This brings up the NE-1 Selector window.

14 Choose the card and port to act as the TAD ports and click OK.

15 Enter the TAP ID value according to vendor requirements and local procedures.

16 Click OK. The Provisioned DS0 TADs appear in the TAP View window. Click Close.

Provisioned DS0 TADs in TAP View



TAP Id	Type	Port	Circuit	Mode
13	DS0_TAD	T1-1-3-3-0-8	-	NONE
14	DS0_TAD	T1-1-3-3-0-8	-	NONE
15	DS0_TAD	T1-1-3-3-0-8	-	NONE
16	DS0_TAD	T1-1-3-3-0-8	-	NONE
17	DS0_TAD	T1-1-3-3-0-8	-	NONE
18	DS0_TAD	T1-1-3-3-0-8	-	NONE
19	DS0_TAD	T1-1-3-3-0-8	-	NONE
20	DS0_TAD	T1-1-3-3-0-8	-	NONE
21	DS0_TAD	T1-1-3-3-0-8	-	NONE
22	DS0_TAD	T1-1-3-3-0-8	-	NONE
23	DS0_TAD	T1-1-3-3-0-8	-	NONE
24	DS0_TAD	T1-1-3-3-0-8	-	NONE

17 This procedure is complete.

The following procedure provides the steps for deleting a TAD.

Deleting a TAD

At the MG 9000 Manager

1 At the Shelf View, go to the Services menu and select DTA Test Manager.

2 At the TAP View, verify that there is currently not a test access (MONEF or SPLTEF) on either TAP of the TAD to be deleted. Select one row of the TAD to be deleted. The 12 TAD entries are adjacent to one another.

3 Click Delete TAP. The TAPs are removed.

4 Click Close.

5 This procedure is complete.

Operating line cut-off relay

Purpose of this procedure

This procedure provides steps on activating, querying, and deactivating the line cut-off relay. The cut-off relay may be used by technicians to isolate an individual line circuit, or group of circuits, from the external facility to prevent damage to the circuit and as over-voltage protection when it is necessary to test the line circuit with a metallic connection.

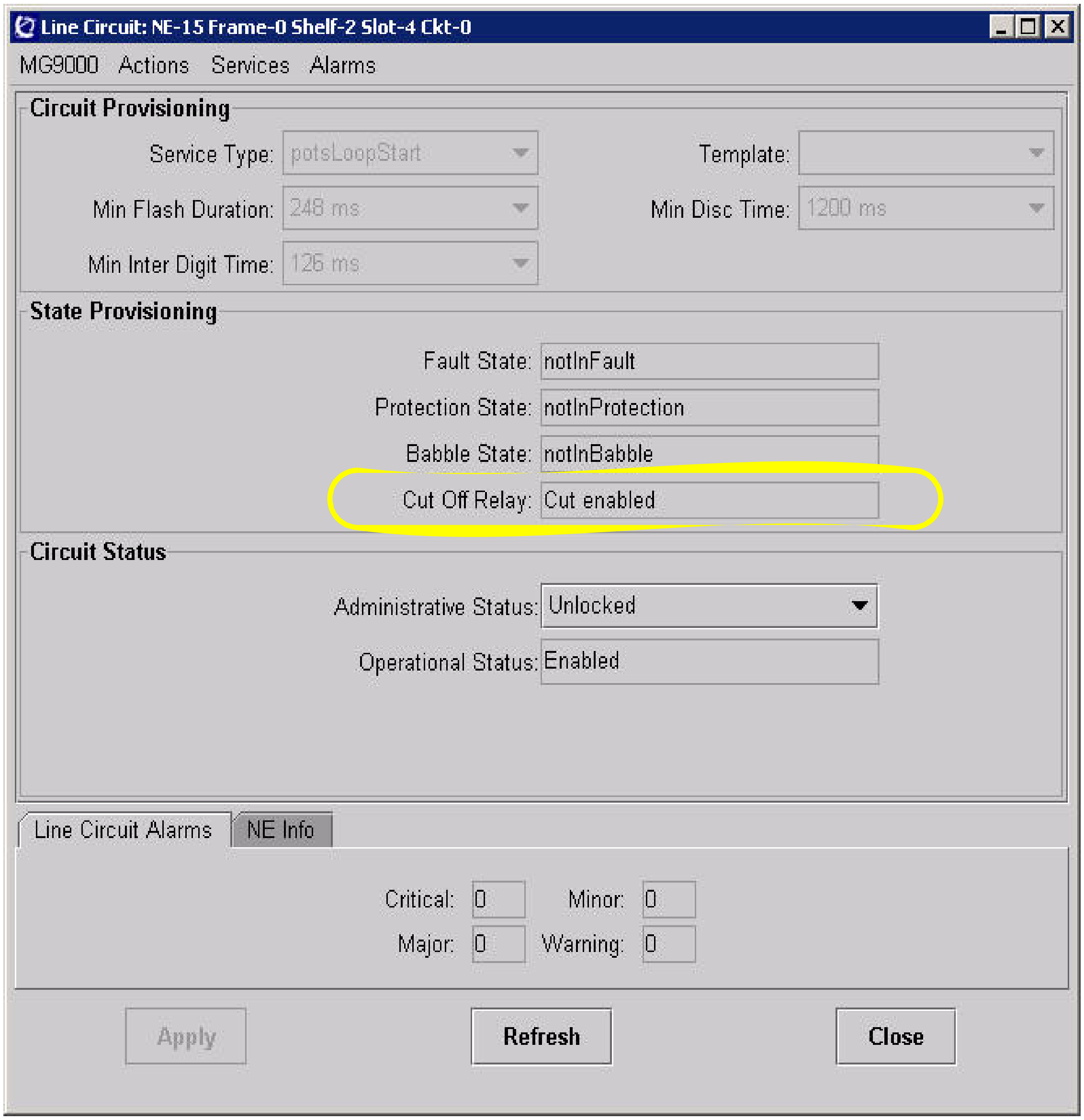
> ***Note:*** When activating the line cut-off relay for a circuit, call processing cannot take place on that circuit.

The Line Circuit View reports the state of the cut-off relay in the Cut Off Relay field in the State Provisioning pane of the window. The two states reported are

- Normal - the cut-off relay is not enabled
- Cut Enabled - the cut-off relay is operated

The following figure shows the Line Circuit View pointing out the Cut Off Relay field. The state of the field is not updated dynamically. To update the state of the cut-off relay on the selected circuit, click on Refresh.

Circuit View showing Cut Off Relay field



Circuit Provisioning

Service Type: potsLoopStart

Template:

Min Flash Duration: 248 ms

Min Disc Time: 1200 ms

Min Inter Digit Time: 126 ms

State Provisioning

Fault State: notInFault

Protection State: notInProtection

Babble State: notInBabble

Cut Off Relay: Cut enabled

Circuit Status

Administrative Status: Unlocked

Operational Status: Enabled

Critical: 0

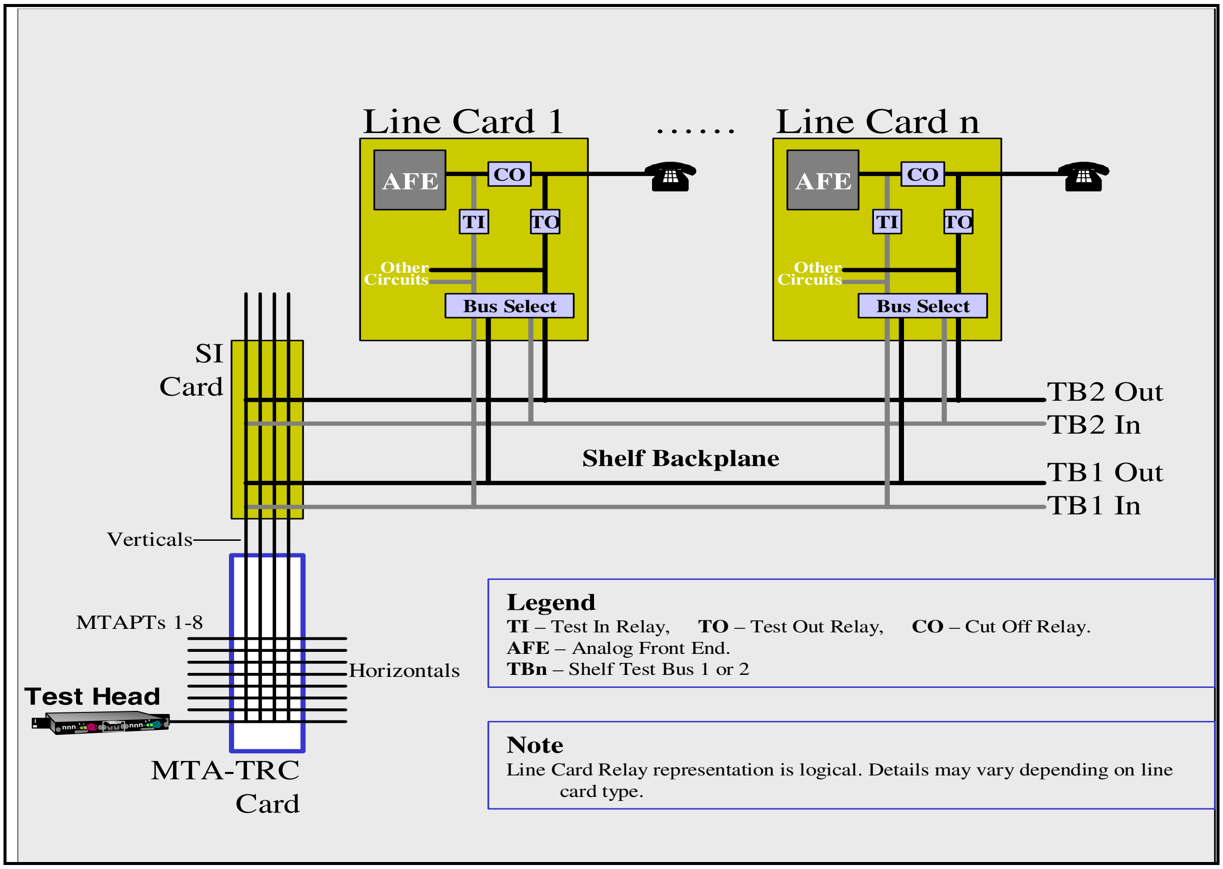
Minor: 0

Major: 0

Warning: 0

The following figure shows the cut-off (CO) relay in each of the supported line card types.

Cut-off relay on line cards



Legend
TI – Test In Relay, **TO** – Test Out Relay, **CO** – Cut Off Relay.
AFE – Analog Front End.
TBn – Shelf Test Bus 1 or 2

Note
Line Card Relay representation is logical. Details may vary depending on line card type.

The following procedures are provided:

- activating the line cut-off relay
- querying the lines in cut-off
- deactivating the line cut-off relay

When to use this procedure

These procedures are used when it is necessary to isolate the line from the loop.

Prerequisites

This procedure has the following prerequisites:

- the line circuit must be discovered
- the line circuit must be idle (that is, no call processing must be occurring)

Action

Activating the line cut-off relay

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon on which the cut-off relay is to be activated. The Frame View appears.

2 At the Frame View, select the shelf on which the line cut-off relay is to be activated. The Shelf View appears.

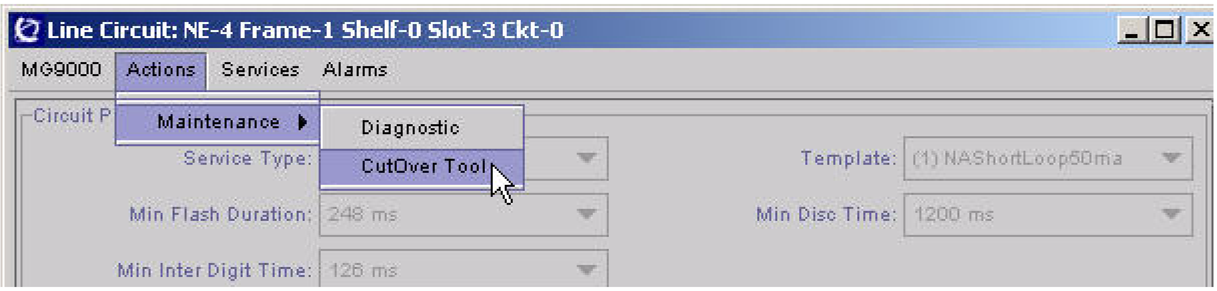
3 At the Shelf View, select the line card on which the circuit or circuits reside that are to be isolated. The Card View appears.

> ***Note:*** If the lines in a shelf, frame, or entire network element are to be isolated, select the lowest number slot in the shelf.

4 At the Card View, select the line circuit 0. The Circuit View appears.

5 From the Actions->Maintenance menu at the top, select CutOver Tool. The following figure shows the menu selection.

Accessing the CutOver Tool menu



Line Circuit: NE-4 Frame-1 Shelf-0 Slot-3 Ckt-0

Service Type:

Template: (1) NAShortLoop50ma

Min Flash Duration: 248 ms

Min Disc Time: 1200 ms

Min Inter Digit Time: 128 ms

The MG9000 Diagnostics View appears.

6

CAUTION

Loss of call processing ability when cut-off relay is activated

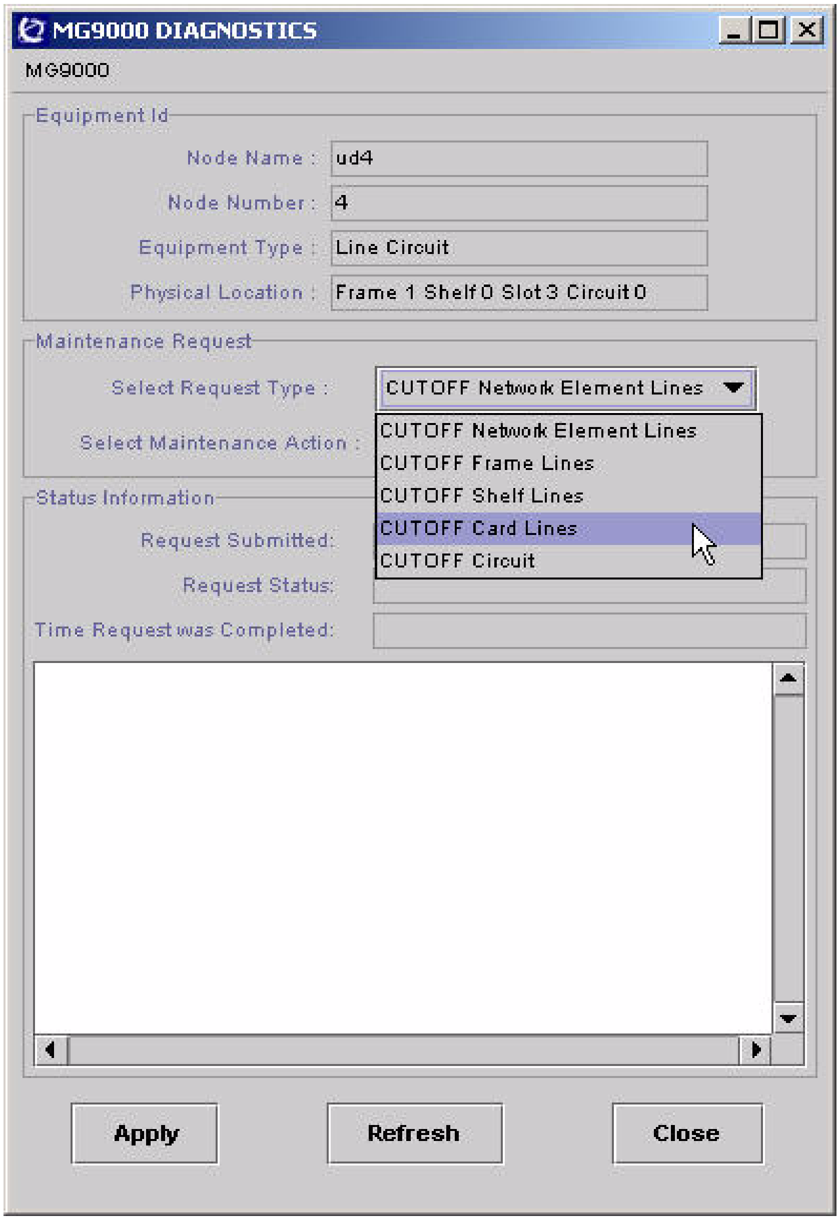
When activating the line cut-off relay for a circuit, call processing cannot take place on that circuit.

In the MG9000 Diagnostics View, in the Maintenance Request pane, use the pull-down menu to select the request type. The following are the types:

- CUTOFF Network Element Lines - activates the cut-off relays for all circuits in the network element
- CUTOFF Frame Lines - activates the cut-off relays for all circuits in the selected frame
- CUTOFF Shelf Lines - activates the cut-off relays for all circuits in the selected shelf
- CUTOFF Card Lines - activates the cut-off relays for all circuits in the selected line card
- CUTOFF Circuit - activates the cut-off relay for the selected circuit

The following figure shows the MG9000 Diagnostics View.

MG9000 Diagnostics View, showing CutOff pull-down menu


MG9000 DIAGNOSTICS

MG9000

Equipment Id

Node Name : ud4

Node Number : 4

Equipment Type : Line Circuit

Physical Location : Frame 1 Shelf 0 Slot 3 Circuit 0

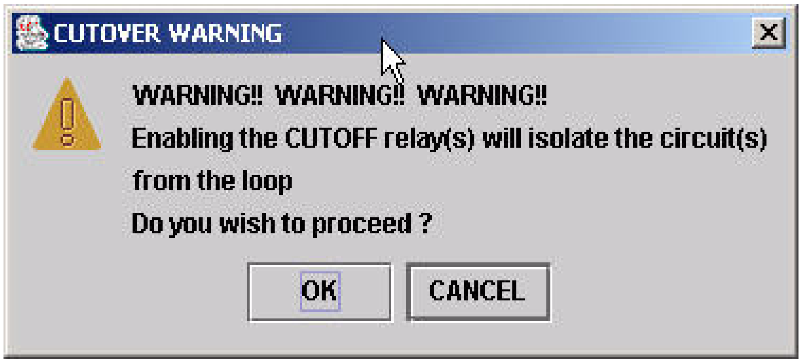
Maintenance Request

Select Request Type : CUTOFF Network Element Lines

7 Select Enable from the Select Maintenance Action pull-down menu.

8 Click Apply at the bottom of the MG9000 Diagnostics View. A warning message will appear as shown in the following figure.

Warning message - enabling cut-off relay



WARNING!! WARNING!! WARNING!!
Enabling the CUTOFF relay(s) will isolate the circuit(s) from the loop
Do you wish to proceed ?

9 Respond to the warning message by clicking on OK.

The Status Information window reports the status of the operation.

10 This procedure is complete.

Querying the lines in cut-off

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon on which the line cut-off is to be queried. The Frame View appears.

2 At the Frame View, select the shelf on which the line cut-off is to be queried. The Shelf View appears.

3 At the Shelf View, select the line card on which the circuit or circuits reside that are to be queried. The Card View appears.

Note: Select the lowest number slot in the shelf.

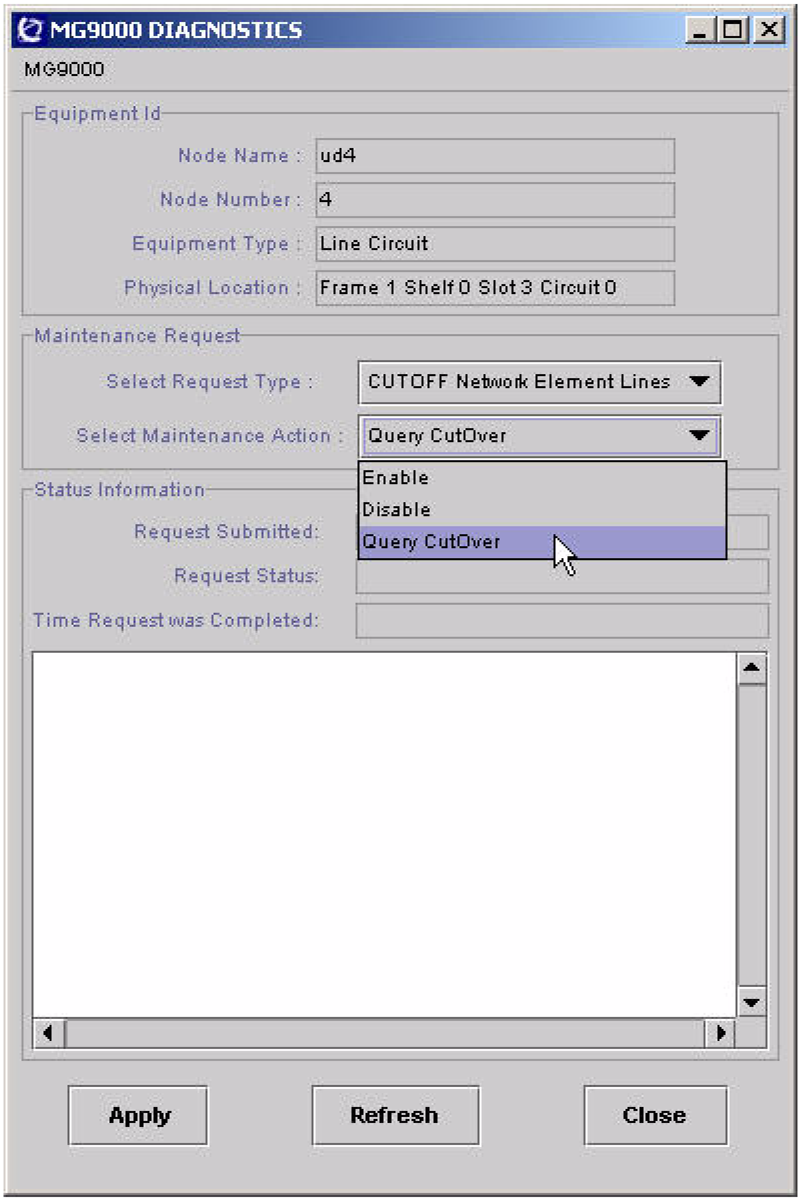
4 At the Card View, select the line circuit 0. The Circuit View appears.

5 From the Actions->Maintenance menu at the top, select CutOver Tool. The MG9000 Diagnostics View appears.

6 In the MG9000 Diagnostics View, in the Maintenance Request pane, use the pull-down menu to select Query Cutover.

The following figure shows the MG9000 Diagnostics View.

MG9000 Diagnostics View, Query Cutover



MG9000 DIAGNOSTICS

MG9000

Equipment Id

Node Name : ud4

Node Number : 4

Equipment Type : Line Circuit

Physical Location : Frame 1 Shelf 0 Slot 3 Circuit 0

Maintenance Request

Select Request Type : CUTOFF Network Element Lines

Select Maintenance Action : Query CutOver

Status Information

Request Submitted:

Request Status:

Time Request was Completed:

7 Click Apply at the bottom of the MG9000 Diagnostics View.

A list of all circuits in cut-off is displayed in the Status Information window.

8 This procedure is complete.

Deactivating the line cut-off relay

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon on which the cut-off relay are activated. The Frame View appears.

2 At the Frame View, select the shelf on which the line cut-off are activated. The Shelf View appears.

3 At the Shelf View, select the line card on which the circuit or circuits reside that are isolated. The Card View appears.

> ***Note:*** If all the lines in a shelf, frame, or entire network element are to be isolated, select the lowest number slot in the shelf.

4 At the Card View, select the line circuit 0. The Circuit View appears.

5 From the Actions->Maintenance menu at the top, select CutOver Tool. The MG9000 Diagnostics View appears.

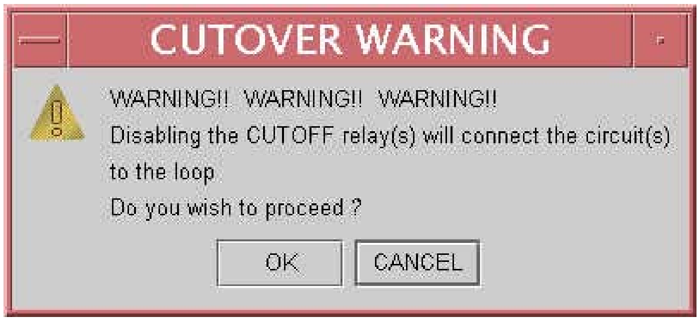
6 In the MG9000 Diagnostics View, in the Maintenance Request pane, use the pull-down menu to select the request type that is to be deactivated. The following are the types:

- CUTOFF Network Element Lines
- CUTOFF Frame Lines
- CUTOFF Shelf Lines
- CUTOFF Card Lines
- CUTOFF Circuit

7 Select Disable from the Select Maintenance Action pull-down menu.

8 Click Apply at the bottom of the MG9000 Diagnostics View. A warning message will appear as shown in the following figure.

Warning message - disabling cut-off relay



CUTOVER WARNING

WARNING!! WARNING!! WARNING!!
Disabling the CUTOFF relay(s) will connect the circuit(s) to the loop
Do you wish to proceed ?

9 Respond to the warning message by clicking on OK.

The Status Information window reports the status of the operation.

10 This procedure is complete.

Fault Correction

This section provides the following procedures for clearing faults by replacing components in the MG 9000.

- Switching activity of a card
- Switching mastership of an ABI card
- Restarting a card
- Locking a card
- Unlocking a card
- Locking a voice or data line circuit
- Unlocking a voice or data line circuit
- Locking an OC3/STS1 carrier path
- Unlocking an OC3/STS1 carrier path
- Locking a GigE port and link
- Unlocking a GigE port and link
- Replacing a cooling unit
- Replacing a Shelf interface card
- Replacing a dual talk battery filter card in an IBIP
- Replacing a Power filter card
- Replacing a current sensor card in an IBIP
- Replacing an alarm relay card in an IBIP
- Replacing an alarm processor card in an IBIP
- Replacing an ITP card
- Replacing a DS1 card
- Replacing an ITX card
- Replacing an MTA-TRC card
- Replacing an ABI card
- Replacing a DCC card
- Replacing an NTTP62 SFP transceiver device
- Replacing a POTS32 line card
- Replacing an SAA card
- Replacing an ADSL 8+8 line card

- Replacing a GLC
- Replacing a fuse in an IBIP
- Replacing an air filter element

Switching activity of a card

Purpose of this procedure

This procedure provides the steps for switching the activity of an active DCC, ITP, or ITX card to an inactive card in the MG 9000 shelf. These cards are provisioned in pairs to support redundancy in the event of a card failure. The calls that are being handled by one card are handed off to the inactive mate card to prevent the loss of service for active calls. This hand-off of calls and services is called a switch of activity or SWACT.

Note: A SWACT can only be performed if the inactive card has an Administrative State of Unlocked and an Operational State of Enabled.

There are two types of SWACT supported:

- manual warm SWACT
- force warm SWACT

Note 1: If a SWACT is successfully performed on a DCC card pair, the newly inactive DCC card will always restart.

Note 2: If a SWACT is successfully performed on an ITX or ITP card pair and there is a fault on the active card for which the activity is being switched away from, the newly inactive card will restart in an attempt to clear the fault.

Note 3: If the inactive card has an Administrative State of Unlocked and an Operational State of Enabled but there is a fault on the inactive card, a manual warm SWACT will not be allowed. A force warm SWACT can be used to force a SWACT to occur.

CAUTION
Ensure the fault scenario on the mate card is understood before proceeding with a force warm SWACT.
Under normal circumstances do not use force warm SWACT. If there is a fault on the inactive card, attempt to clear the fault before attempting a SWACT. Refer to the appropriate fault clearing procedure in this document.

When to use this procedure

Use this procedure when it is necessary to switch the activity of an active card in a maintenance scenario.

Prerequisites

This procedure has no prerequisites.

Action

Switching activity of a card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

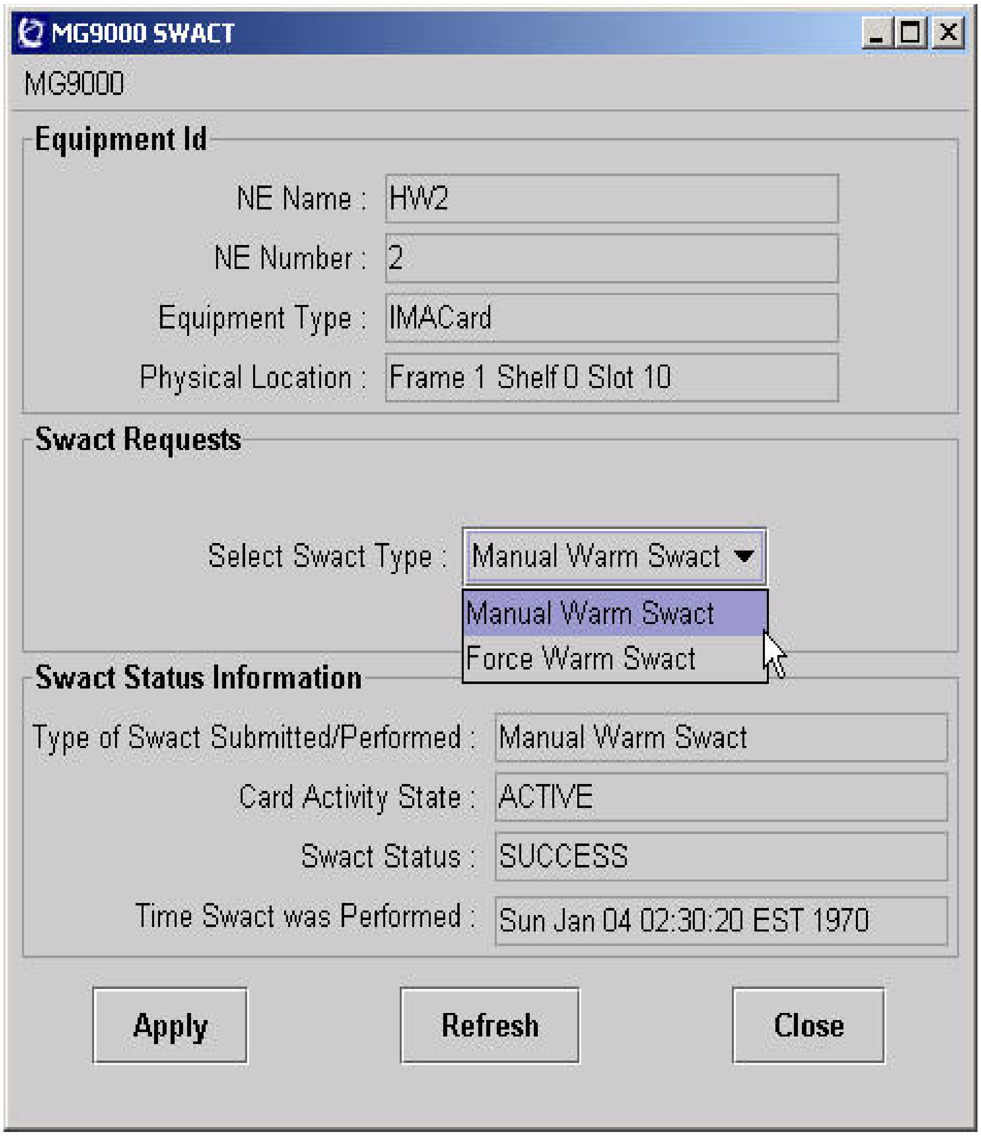
2 In the Frame View, double click on the shelf. The Shelf View appears.

3 Double click on the card to access the Card View for the card type for which activity is to be switched

4 From the Actions menu at the top of the Card View, select Maintenance->Swact. The MG 9000 SWACT View appears. The following figure shows the MG 9000 SWACT View.

5 From the MG 9000 Swact View, select the type of SWACT to be performed, Manual Warm Swact or Force Warm Swact from the Select Swact Type pull-down combo box.

MG 9000 SWACT View



MG9000 SWACT

MG9000

Equipment Id

NE Name : HW2

NE Number : 2

Equipment Type : IMACard

Physical Location : Frame 1 Shelf 0 Slot 10

Swact Requests

Select Swact Type : Manual Warm Swact

Swact Status Information

Type of Swact Submitted/Performed : Manual Warm Swact

Card Activity State : ACTIVE

Swact Status : SUCCESS

Time Swact was Performed : Sun Jan 04 02:30:20 EST 1970

6 Click on Apply to invoke the SWACT.

Wait for the Standby status to change to Hot-Standby.

7 This procedure is complete.

Switching mastership of an ABI card

Purpose of this procedure

This procedure provides the steps for switching mastership of an master ABI card to a slave ABI card in the MG 9000 shelf. The ABI cards are provisioned in pairs to support redundancy in the event of a card failure.

There are two types of Switch Mastership supported:

- manual Switch Mastership
- force Switch Mastership

When to use this procedure

Use this procedure when it is necessary to switch the mastership of an ABI card in a maintenance scenario.

Prerequisites

This procedure has no prerequisites.

Action

Switching mastership of an ABI card

At the MG 9000 Manager

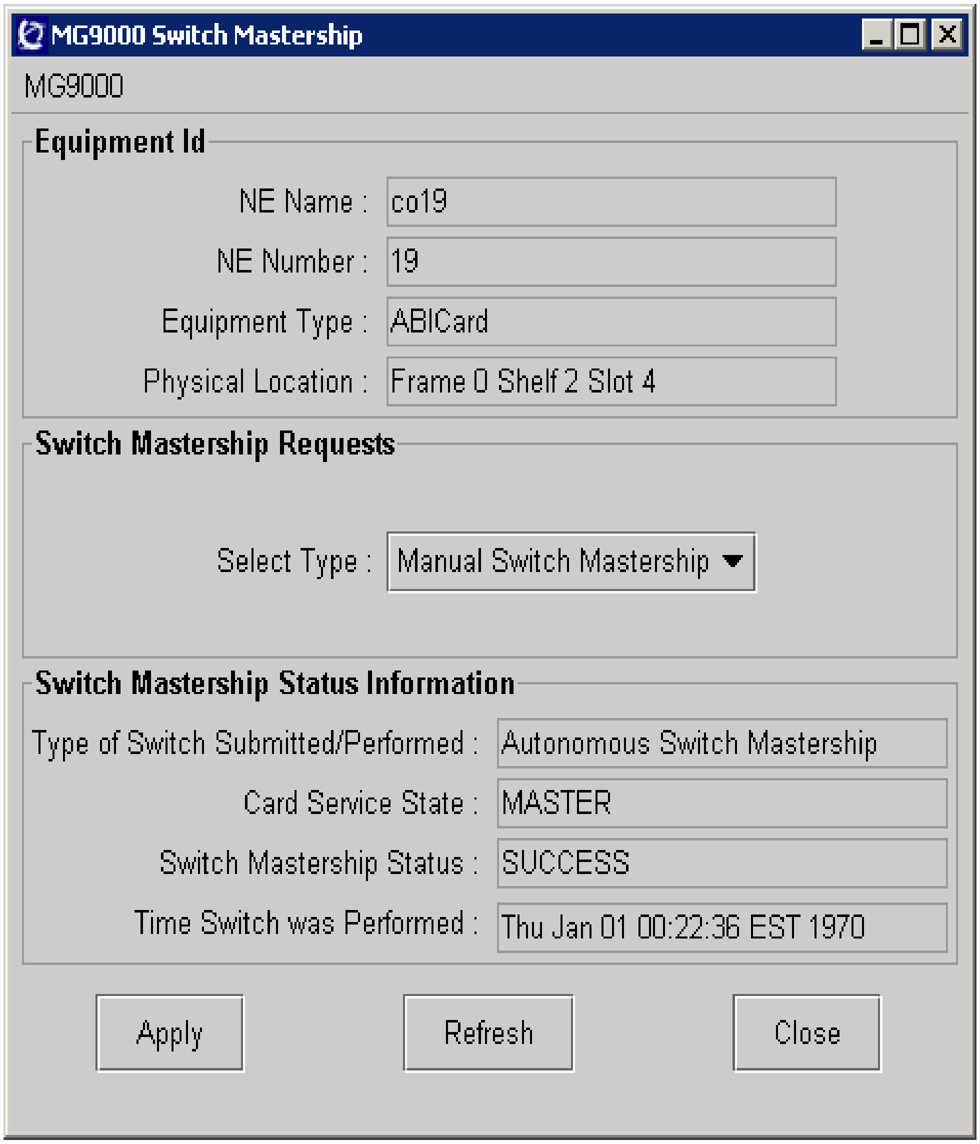
1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 In the Frame View, double click on the shelf. The Shelf View appears.

3 Double click on the ABI card to access the Card View for the ABI card type for which mastership is to be switched.

4 From the Actions menu at the top of the Card View, select Maintenance->Switch Mastership. The MG 9000 Switch Mastership View appears. The following figure shows the MG 9000 Switch Mastership View.

MG 9000 Switch Mastership View



MG9000 Switch Mastership

MG9000

Equipment Id

NE Name : co19

NE Number : 19

Equipment Type : ABICard

Physical Location : Frame 0 Shelf 2 Slot 4

Switch Mastership Requests

Select Type : Manual Switch Mastership

Switch Mastership Status Information

Type of Switch Submitted/Performed : Autonomous Switch Mastership

Card Service State : MASTER

Switch Mastership Status : SUCCESS

Time Switch was Performed : Thu Jan 01 00:22:36 EST 1970

5 From the MG 9000 Switch Mastership View, select the type of Switch to be performed, Manual Switch Mastership or Force Switch Mastership from the Select Type pull-down combo box.

6 Click on Apply to invoke the Switch Mastership.

Wait for the Status to change to Providing_Service_Slave.

7 This procedure is complete.

Restarting a card

Purpose of this procedure

This procedure provides the steps for restarting a DS1, ITP, ITX, DCC (OC-3/DS1-IMA/GigE), ADSL, or DS-512 (ABI) card.

The following types of restarts are supported:

- restarting an ADSL card
  - restart current cold
  - restart current unconditional
  - restart current warm
- restarting a DS1, ITP, ITX, ABI, or DCC (OC-3/DS1-IMA/GigE) card
  - restart current
  - restart flash primary
  - restart flash backup

When to use this procedure

Use this procedure when it is necessary to restart a DS1, ITP, ITX, DCC (OC-3/DS1-IMA/GigE), ADSL, or DS-512 card in a maintenance scenario.

Use the Restart Current Warm command to restart the DSP on the ADSL card to recover a DSP lockup condition without affecting calls.

Prerequisites

This procedure has no prerequisites.

Action

Restarting a card

At the MG 9000 Manager

1. At the Subnet View, double click the MG 9000 icon. The Frame View appears.
2. In the Frame View, double click on the shelf. The Shelf View appears.
3. Double click on the card to access the Card View for the card type for which activity is to be switched.
4. Lock the card using the Locking a card procedure.

5 Select the restart type to be performed in the Card pane of the card view.

6 Click Restart. The restart status is reported in the bottom text banner in the card view.

7 This procedure is complete.

Locking a card

Purpose of this procedure

This procedure provides the steps for locking a card in the MG 9000 shelf.

> ***Note:*** When locking cards that has calls in progress, the system will deny a request to lock the card. The denial can be overridden by using the Force Lock and active calls will be taken down.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a card from unlock to lock as part of a maintenance activity.

Prerequisites

The Administrative state of the card must be unlocked.

Action

Locking a card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 In the Frame View, double click on the shelf. The Shelf View appears.

3 Double click on the card to access the Card View for the card type to be taken out of service.

4 Use the following table to determine the next step.

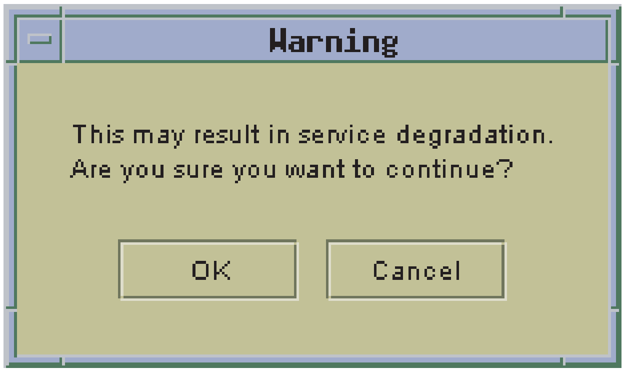
If the card is	Do
a DCC, ITP, or ITX and is Active	step 5
a DCC, ITP, or ITX and is not active	step 9
an ABI (DS-512) card and is the Master card	step 7
an ABI (DS-512) card and is the Slave card	step 8
a DS1 card	step 6
a line card (SAA, POTS 32, GLC 32, or xDSL)	step 9

5 To switch the activity of the currently active DCC, ITP, or ITX card to be inactive, from the Actions menu at the top of the Card View, select Maintenance->SWACT. Wait for the Standby status to change to Hot_Standby. Go to step 9

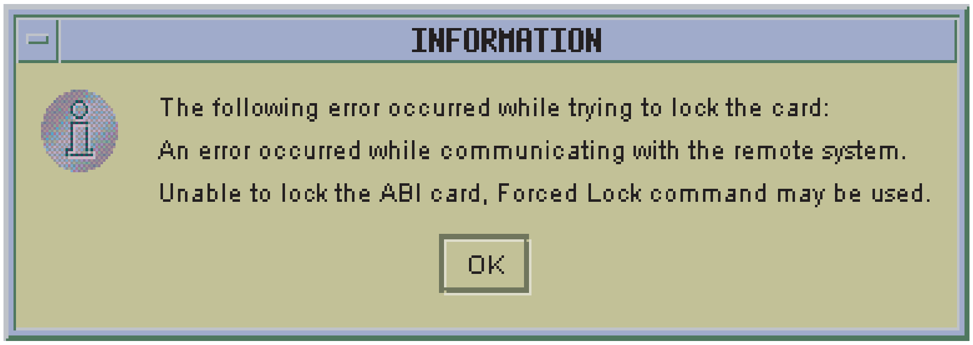
6 If the card to be locked is a DS1 card, go to step 9.

7 If the card to be locked is a Master ABI card, perform a Switch Mastership to switch mastership of the ABI card. Go to the Switching mastership of an ABI card procedure and return to this step. After the Master ABI Service Status is Providing_Service_Slave, go to step 8.

8 If the card to be locked is a Slave ABI card, a warning message will appear and an informational message will appear warning of service degradation when the Slave ABI card is taken out of service. The warning and information messages are shown next.


Warning

This may result in service degradation.
Are you sure you want to continue?


INFORMATION

The following error occurred while trying to lock the card:
An error occurred while communicating with the remote system.
Unable to lock the ABI card, Forced Lock command may be used.

To continue with locking the Slave ABI card, use the Force Lock option.

Go to step 10.

9

CAUTION
Loss of service
If calls are in progress, the lock will fail. Attempt to lock the card later or use the Force option to drop all calls in progress.

To lock the card, change the Administrative state by selecting Lock.

10 This procedure is complete.

Unlocking a card

Purpose of this procedure

This procedure provides the steps for unlocking a card in the MG 9000 shelf.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a card from lock to unlock.

Prerequisites

The card must be in the Locked Administrative state.

Action

Unlocking a card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 In the Frame View, double click on the shelf. The Shelf View appears.

3 Double click on the cards to access the Card View for the card type that is to be returned to service.

4 To unlock the card, change the Administrative state by selecting Unlocked. Wait for the pop-up message to appear indicating the card has returned to service.

5 This procedure is complete.

Locking a voice or data line circuit

Purpose of this procedure

This procedure provides the steps for locking a voice or data line circuit connected to a line card in the MG 9000 shelf. A warning message appears that says: If in-service terminations exist on the circuit, services may be disrupted.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a voice or data line circuit from unlock to lock as part of a maintenance activity.

Prerequisites

The Administrative state of the card must be unlocked.

Action

Locking a voice or data line circuit

At the MG 9000 Manager

1 At the Subnet View, double click on the MG 9000 icon. The Frame View appears.

2 In the Frame View, double click on the shelf containing the card to which the line circuit to be Locked is connected.

3 Identify and double click on the card which has the circuit(s) that are to be locked.

4 Use the information in the following table to determine the next step.

If	Do
one circuit on the line card is to be locked	step 5
multiple circuits on the line card are to be locked	step 7

5 From the Card View, double click on the individual circuit. The Circuit View appears.

6 From the Circuit View, in the Status pane, change the Administrative Status to Locked and reply to the warning

message. If there is a call in progress and the circuit must be locked, use Forced lock.

> ***Note:*** If Forced Lock is used, and a call is in progress on the circuit to be locked, the call will be taken down. Perform this activity during a period of low traffic to avoid a loss of service.

Go to step 10.

7 From the Card View, select Services->Circuits Listing from the menu bar. The Circuits Listing screen appears.

8 Click on the first circuit to be locked and then hold down the Ctrl key and click to select additional circuits to be locked.

> ***Note:*** If a sequential group of circuits must be selected, select the first circuit then hold the Shift key and click on the last circuit.

9 In the Set Values pane, click on the Lock radio button then click Apply to submit the action and reply to the warning message.

10 This procedure is complete.

Unlocking a voice or data line circuit

Purpose of this procedure

This procedure provides the steps for unlocking a voice or data line circuit connected to a line card in the MG 9000 shelf.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a voice or data line circuit from lock to unlock.

Prerequisites

The Administrative state of the card must be locked.

Action

Unlocking a voice or data line circuit

At the MG 9000 Manager

1 At the Subnet View, double click on the MG 9000 icon. The Frame View appears.

2 In the Frame View, double click on the shelf containing the card to which the line circuit to be unlocked is connected.

3 Identify and double click on the card which has the circuit(s) that are to be unlocked.

4 Use the information in the following table to determine the next step.

If	Do
one circuit on the line card is to be unlocked	step 5
multiple circuits on the line card are to be unlocked	step 7

5 From the Card View, double click on the individual circuit. The Circuit View appears.

6 From the Circuit View, in the Status pane, change the Administrative Status to Unlocked and click Apply. Go to step 10.

7 From the Card View, select Services->Circuits Listing from the menu bar. The Circuits Listing screen appears.

8 Click on the first circuit to be unlocked and then hold down the Ctrl key and click to select additional circuits to be unlocked.

Note: If a sequential group of circuits must be selected, select the first circuit then hold the Shift key and click on the last circuit.

9 In the Set Values pane, click on the Unlock radio button then click Apply to submit the action and reply to the warning message.

10 This procedure is complete.

Locking an OC3/STS1 carrier path

Purpose of this procedure

This procedure provides the steps for locking an OC3/STS1 carrier path of a channelized OC3 carrier.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a port to locked as part of a maintenance activity.

Prerequisites

The Administrative state of the card may be unlocked.

Action

Locking an OC3/STS1 carrier path

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 In the Frame View, double click on the shelf. The Shelf View appears.

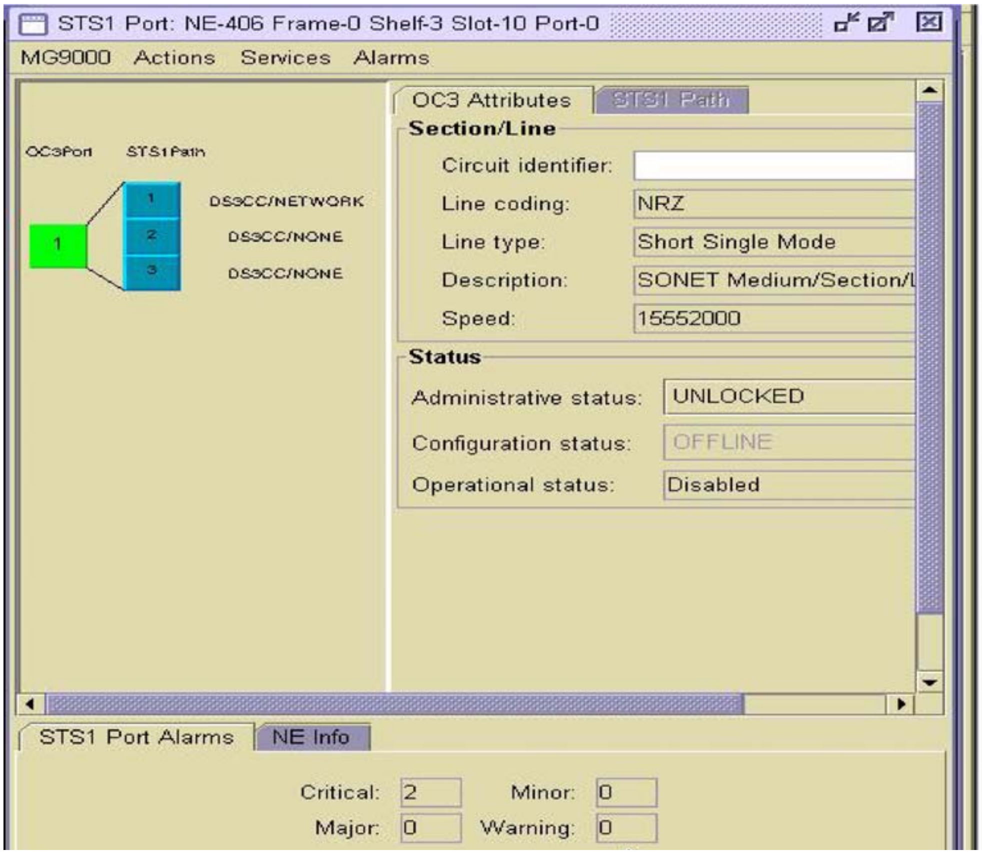
3 Double click on the OC3 card to access the Card View.

4 Double click on the OC3Port icon. The OC3 Port View appears.

5 The next step is based on information in the following table.

If the carrier is	Do
concatenated, the OC3 carrier is used as a single ATM pipe and only the entire port can be locked	step 10
channelized, as noted by the three icons for the STS1 path in the OC3 Port View	step 6

6 The following figure shows a channelized carrier and the path icons. Three STS1 path icons are adjacent to the OC3port icon.



Section/Line

Circuit identifier:

Line coding: NRZ

Line type: Short Single Mode

Description: SONET Medium/Section/L

Speed: 15552000

Status

Administrative status: UNLOCKED

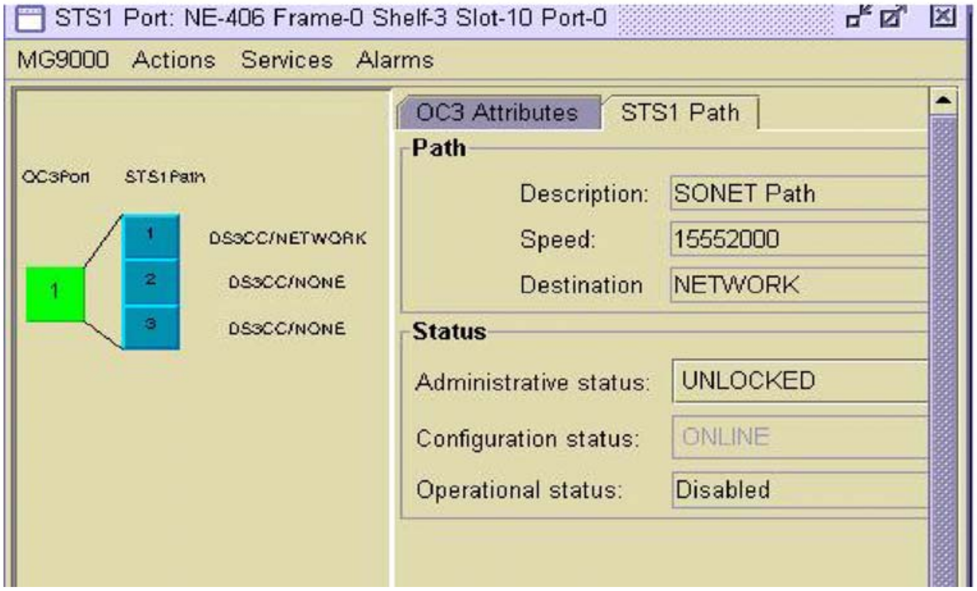
Configuration status: OFFLINE

Operational status: Disabled

Critical: 2 Minor: 0

Major: 0 Warning: 0

7 Double click on an STS1 path to display STS1 path information and its status in the STS1 Path tab on the right side of the port view. The following figure shows the STS1 path description and status information.



STS1 Port: NE-406 Frame-0 Shelf-3 Slot-10 Port-0

Path

Description: SONET Path

Speed: 15552000

Destination NETWORK

Status

Administrative status: UNLOCKED

Configuration status: ONLINE

Operational status: Disabled

8 Change the Administrative status of the STS1 path by selecting Locked.

9 Select the OC3 Attributes tab and change the Administrative status of the OC3 port by selecting Locked.

10 This procedure is complete.

Unlocking an OC3/STS1 carrier path

Purpose of this procedure

This procedure provides the steps for unlocking an OC3/STS1 carrier path of a channelized OC3 carrier.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a port to locked as part of a maintenance activity.

Prerequisites

The Administrative state of the card must be locked.

Action

Unlocking an OC3/STS1 carrier path

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 In the Frame View, double click on the shelf. The Shelf View appears.

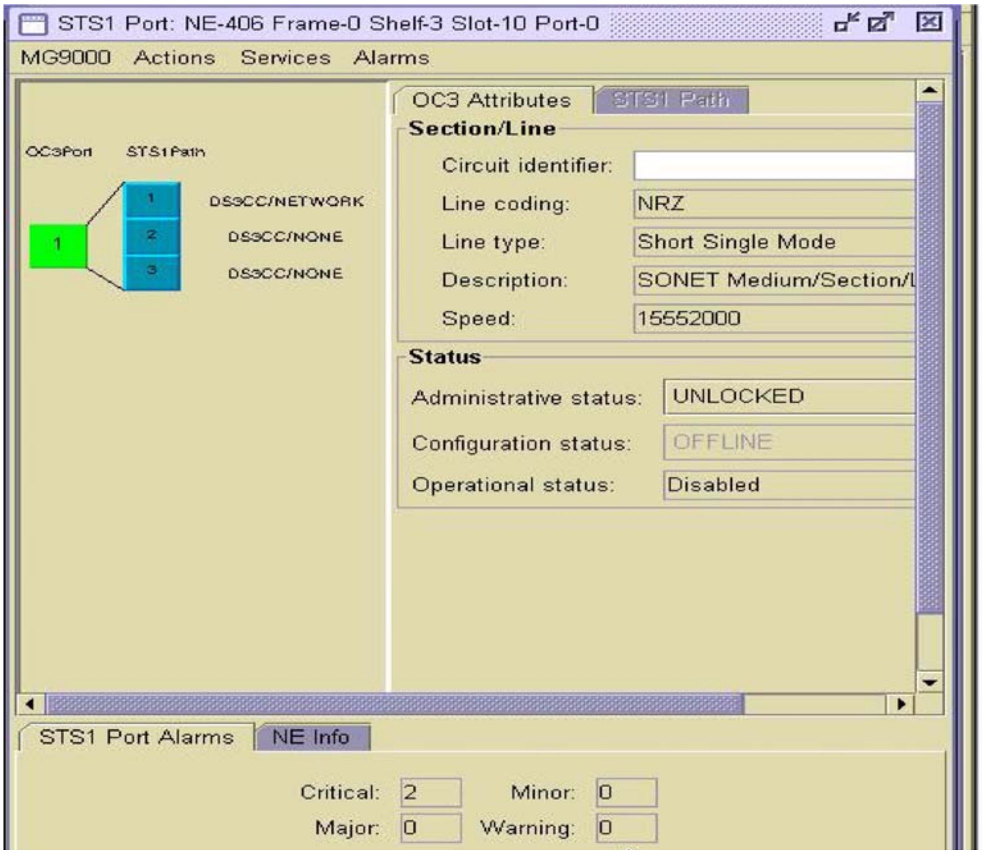
3 Double click on the OC3 card to access the Card View.

4 Double click on the OC3Port icon. The OC3 Port View appears.

5 The next step is based on information in the following table.

If the carrier is	Do
concatenated, the OC3 carrier is used as a single ATM pipe and only the entire port can be locked	step 10
channelized, as noted by the three icons for the STS1 path in the OC3 Port View	step 6

6 The following figure shows a channelized carrier and the path icons. Three STS1 path icons are adjacent to the OC3port icon.



Section/Line

Circuit identifier:

Line coding: NRZ

Line type: Short Single Mode

Description: SONET Medium/Section/L

Speed: 15552000

Status

Administrative status: UNLOCKED

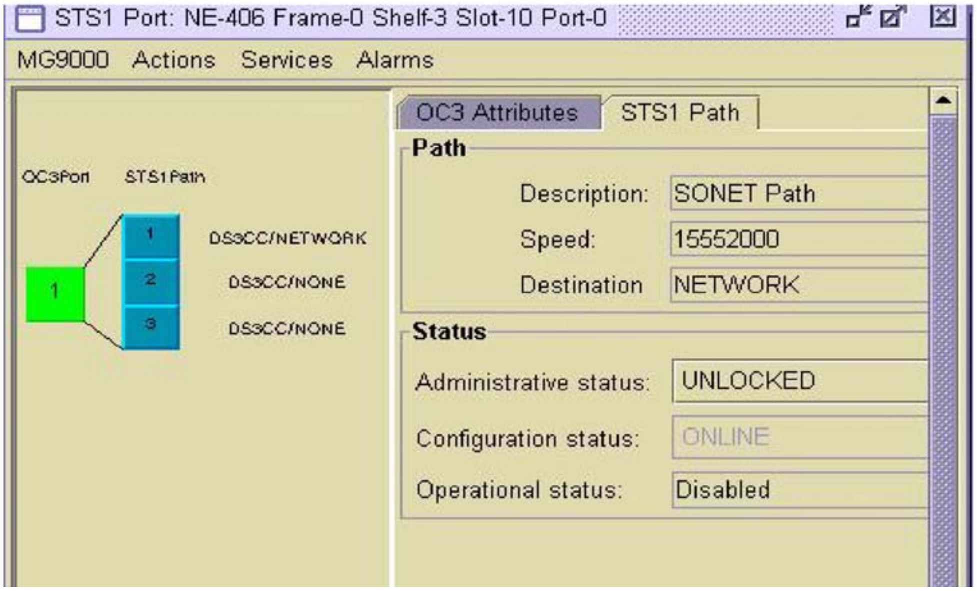
Configuration status: OFFLINE

Operational status: Disabled

Critical: 2 Minor: 0

Major: 0 Warning: 0

7 Double click on an STS1 path to display STS1 path information and its status in the STS1 Path tab on the right side of the port view. The following figure shows the STS1 path description and status information.



STS1 Port: NE-406 Frame-0 Shelf-3 Slot-10 Port-0

MG9000 Actions Services Alarms

Path

Description: SONET Path

Speed: 15552000

Destination NETWORK

Status

Administrative status: UNLOCKED

Configuration status: ONLINE

Operational status: Disabled

8 Select the OC3 Attributes tab and change the Administrative status of the OC3 port by selecting Unlocked.

9 Select the STS1 Path tab and change the Administrative status by selecting Unlocked.

10 This procedure is complete.

Locking a GigE port and link

Purpose of this procedure

This procedure provides the steps for locking a GigE port and link.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a GigE port to locked as part of a maintenance activity.

Prerequisites

The Administrative state of the NTNY45FA GigE DCC card must be unlocked.

Action

Locking a GigE port and link

At the MG 9000 Manager

1 From the Shelf View, double click on the inactive GigE DCC card in the master shelf. The GigE Card view appears.

2 From the GigE Card view, double click on the GigE Port 0 icon. The GigE Port view appears.

3 Click on the Link Controls tab.

4 Select locked from the Administrative Status pull down menu.

5 This procedure is complete.

Unlocking a GigE port and link

Purpose of this procedure

This procedure provides the steps for unlocking a GigE port and link.

When to use this procedure

Use this procedure when it is necessary to change the Administrative state of a GigE port to locked as part of a maintenance activity.

Prerequisites

The Administrative state of the NTNY45FA GigE DCC card must be locked.

Action

Unlocking a GigE port and link

At the MG 9000 Manager

1. From the Shelf View, double click on the inactive GigE DCC card in the master shelf. The GigE Card view appears.
2. From the GigE Card view, double click on the GigE Port 0 icon. The GigE Port view appears.
3. Click on the Link Controls tab.
4. Select Unlocked from the Administrative Status pull down menu.
5. This procedure is complete.

Replacing a cooling unit

Purpose of this procedure

Use the instructions in the procedure that follows to replace a faulty NTNY18 cooling unit.

When to use this procedure

Use this procedure when an NTNY18 cooling unit fails.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a cooling unit

At the MG 9000 equipment frame

1

> **CAUTION**
>
> **Risk of overheating**
>
> Prolonged use of the system while replacing the NTNY18 8-fan cooling unit may cause the equipment in the frame to overheat.
>
> Perform replacement of cooling unit in a timely manner. Review the steps of this procedure to ensure all tools and parts necessary to complete the task are available before the beginning of the procedure.

Obtain a replacement cooling unit. Make sure the replacement cooling unit and the unit you replace have the same PEC and PEC suffix.

2 Remove the cooling unit front cover by pulling it free of the four posts that hold it to the four holding clips.

3 Remove the fuse modules on the IBIP fuse panel that supply power to the cooling unit being replaced. CU0-A and CU0-B supply power to cooling unit 0 (lower). CU1-A and CU1-B supply power to cooling unit 1 (upper).

Note: Return power to the cooling units in a timely manner to prevent equipment damage because of overheating.

4 Remove the power connectors to the cooling unit to be replaced.

5 Remove the screws that hold the cooling unit in place.

6 Pull the cooling unit out until it is free of the frame.

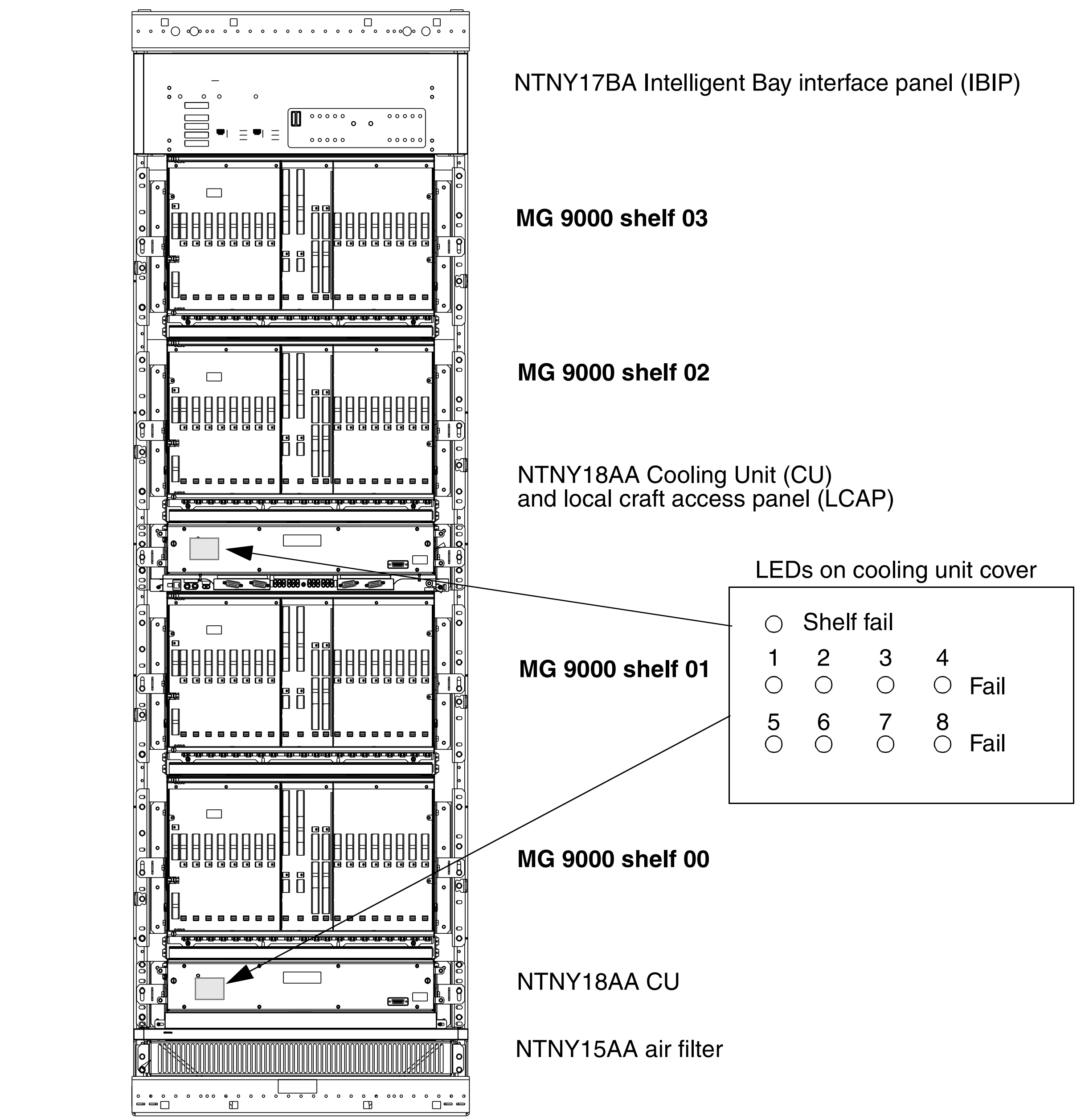
7 Install the replacement cooling unit into the frame. Replace the screws that were removed in step 5 to secure the cooling unit to the frame.

8 Replace the fuse modules for the cooling unit that were removed in step 3.

9 A red LED will light briefly on the face of the cooling unit and then go out, indicating proper connection.

10 Check that the LED does not remain lit and that the fans are operating properly by the absence of any lit fan LEDS on the face of the cooling unit. Refer to the following figure to locate the LEDs on the cooling unit.

MG 9000 frame and cooling unit LEDs



11 Replace the cooling unit front cover. Align the four posts on the cooling unit to the holding clips on the back of the front cover. Lightly strike each end of the front cover with one hand until the cover snaps into place.

12 Return the cooling unit for repair or replacement according to local procedures.

13 This procedure is complete.

Replacing an NTNY23 Shelf interface card

Purpose of this procedure

The following procedure provides the steps for replacing an NTNY23 shelf interface card (SIC) which resides in top half of slot 1 in the MG 9000 shelf.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a SIC card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a Shelf interface card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2

> **CAUTION**
> **Loss of service**
> Replacing the SIC card requires that the MG 9000 shelf be in a stable, non-transitional state.

Double click on the shelf to access the Shelf View for the MG 9000 shelf with the faulty SIC card to be replaced.

Note: During the SIC replacement, no alarms or external audible or scan points are reported on the shelf the SIC card is removed.

3 Identify the SIC card with the alarm condition by observing the alarm balloon.

4 Double-click on the SIC card to access the SIC Card View. The SIC Card View appears.

5 To lock the SIC card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the State pane. Set the Configuration State to Offline from the configuration state pull-down menu in the State pane. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

6

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement SIC card having the same PEC and suffix as the card being replaced.

7 Carefully disconnect the connectors on the faceplate of the SIC card. Carefully lay the cables aside.

8 Remove the screws that secure the SIC in the slot.

9

> **WARNING**
> **Equipment damage**
> Ensure the red “OK to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty SIC card in the frame, shelf, and slot number identified in the Shelf View screen on the MG 9000 Manager.

10 Secure the SIC card in the slot using the screws removed in step 8.

11 Carefully reconnect the connectors that were disconnected in step 7.

12 To return the SIC card to service, set the Configuration state to Online from the configuration state pull-down menu in the State pane. Set the Administrative state to Unlocked from the administrative state pull-down menu in the State pane.

13 Return the card for repair or replacement according to local procedures.

14 This procedure is complete.

Replace a dual talk battery filter card in an IBIP

Purpose of this procedure

Use the following procedure to replace the NTNY25BA dual talk battery filter card.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a dual talk battery filter card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a dual talk battery filter card in an IBIP

At your current location

1 Proceed only if you have been directed to this card replacement procedure by your maintenance support group.

At the MG 9000 Manager

2 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

3 Double click on the IBIP shelf to access the IBIP Shelf View for the MG 9000 IBIP shelf with the faulty IBPTD card.

4 Identify the dual talk battery filter card (IBPTD) with the alarm condition by observing the alarm balloon then double-click on the faulty card to access the IBPDT Card View. The IBPDT Card View appears.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the state section. Refer to Locking a card.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. Wait for the Restart to complete. Observe that the LED indicator on the Card View changes to red, indicating “Safe to pull.”

At the MG 9000 frame

7 Obtain a replacement card. Verify that the replacement card has the same product equipment code (PEC), including suffix, as the card that is to be removed.

8 Remove the BIP front cover.

Note: The IBPTD card should always be engaged and disengaged from a powered up BIP for proper circuit reset and fast discharge of the dual talk battery filter card's capacitors.

9

WARNING
Static electricity damage
Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

DANGER
Risk of electrical shock
To avoid possible shock hazard when removing the dual talk battery filter card, handle the card only by the faceplate. Risk of electrical shock is no longer present after 3 minutes, at which time the internal capacitor has fully discharged.

DANGER
Risk of equipment damage
Do not place the dual talk battery filter card on a conductive surface, as it contains a large capacitor that can discharge. Place the card on a nonconducting surface for 3 minutes until the capacitor has had a chance to fully discharge internally.

Do not reinsert the same card until it has had a chance to fully discharge, which takes approximately 3 minutes. Reinserting a card that has not fully discharged may cause voltage transients on the talk battery leads.

Loosen the hold-down screw on the faceplate of the dual talk battery filter card.

10 Hold the card by its faceplate and carefully remove the card from the IBIP. Do not place the card on a conductive surface.

11 Insert a replacement card into the IBIP and fasten the card into place with the hold-down screw.

12 Replace the IBIP front cover.

At the MG 9000 Manager

13 To return the IBPTD card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section, wait for the Restart to complete, and set the Administrative state to Unlocked from the administrative state pull-down menu in the state section.

14 Return the card for repair or replacement according to local procedures.

15 The procedure is complete.

Replacing an NTNY26 Power filter card

Purpose of this procedure

The following procedure provides the steps for replacing an NTNY26 power filter card (PFC) which resides in bottom half of slot 1 in the MG 9000 shelf.

When to use this procedure

Use this procedure when the Fuse Fail LED is lit on the PFC indicating a PFC card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a Power filter card

At your current location

1 Proceed only if you have been directed to this card replacement procedure by your maintenance support group.

At the MG 9000 frame

2

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Obtain a replacement card. Verify that the replacement card has the same product equipment code (PEC), including suffix, as the card that is to be removed.

3 Remove the screws that secure the PFC in the slot.

4 Replace the faulty PFC card.

5 Secure the PFC card in the slot using the screws removed in step 3.

6 Return the card for repair or replacement according to local procedures.

7 This procedure is complete.

Replace a current sensor card in an IBIP

Purpose of this procedure

Use the following procedure to replace the NTNY27 current sensor card.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a current sensor card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a current sensor card in an IBIP

At your current location

1 Proceed only if you have been directed to this card replacement procedure by your maintenance support group.

At the MG 9000 Manager

2 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

3 Double click on the IBIP shelf to access the IBIP Shelf View for the MG 9000 IBIP shelf with the faulty alarm relay card.

4 Identify the alarm relay card with the alarm condition by observing the alarm balloon.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the state section. Refer to Locking a card.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. Wait for the Restart to complete. Observe that the LED indicator on the Card View changes to red, indicating “Safe to pull.”

At the MG 9000 frame

7 Obtain a replacement card. Verify that the replacement card has the same product equipment code (PEC), including suffix, as the card that is to be removed.

8 Remove the IBIP front cover.

9

WARNING

Static electricity damage

Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Loosen the hold-down screw on the faceplate of the current sensor card.

10 Hold the current sensor card by its faceplate and carefully remove the card from the IBIP.

11 Insert a replacement current sensor card into the IBIP and fasten the card into place with the hold-down screw.

12 Replace the IBIP front cover.

At the MG 9000 Manager

13 To return the current sensor card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section, wait for the Restart to complete, and set the Administrative state to Unlocked from the administrative state pull-down menu in the state section.

14 Return the card for repair or replacement according to local procedures.

15 The procedure is complete.

Replace an alarm relay card in an IBIP

Purpose of this procedure

Use the following procedure to replace the NTNY28 alarm relay card.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating an alarm relay card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an alarm relay card in an IBIP

At your current location

1 Proceed only if you have been directed to this card replacement procedure by your maintenance support group.

At the MG 9000 Manager

2 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

3 Double click on the IBIP shelf to access the IBIP Shelf View for the MG 9000 IBIP shelf with the faulty alarm relay card.

4 Identify the alarm relay card with the alarm condition by observing the alarm balloon.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the state section. Refer to Locking a card.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. Wait for the Restart to complete. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

7 Obtain a replacement card. Verify that the replacement card has the same product equipment code (PEC), including suffix, as the card that is to be removed.

8 Remove the IBIP front cover.

9

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Loosen the hold-down screw on the faceplate of the alarm relay card.

10 Hold the alarm relay card by its faceplate and carefully remove the card from the IBIP.

11 Insert a replacement alarm relay card into the IBIP and fasten the card into place with the hold-down screw.

12 Replace the IBIP front cover.

At the MG 9000 Manager

13 To return the alarm relay card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section, wait for the Restart to complete, and set the Administrative state to Unlocked from the administrative state pull-down menu in the state section.

14 Return the card for repair or replacement according to local procedures.

15 The procedure is complete.

Replace an alarm processor card in an IBIP

Purpose of this procedure

Use the following procedure to replace an NTNY29 alarm processor card.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating an alarm processor card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an alarm processor card in an IBIP

At your current location

1 Proceed only if you have been directed to this card replacement procedure by your maintenance support group.

At the MG 9000 Manager

2 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

3 Double click on the IBIP shelf to access the IBIP Shelf View for the MG 9000 IBIP shelf with the faulty alarm processor card.

4 Identify the alarm processor card with the alarm condition by observing the alarm balloon.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the state section. Refer to Locking a card.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. Wait for the Restart to complete. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

7

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

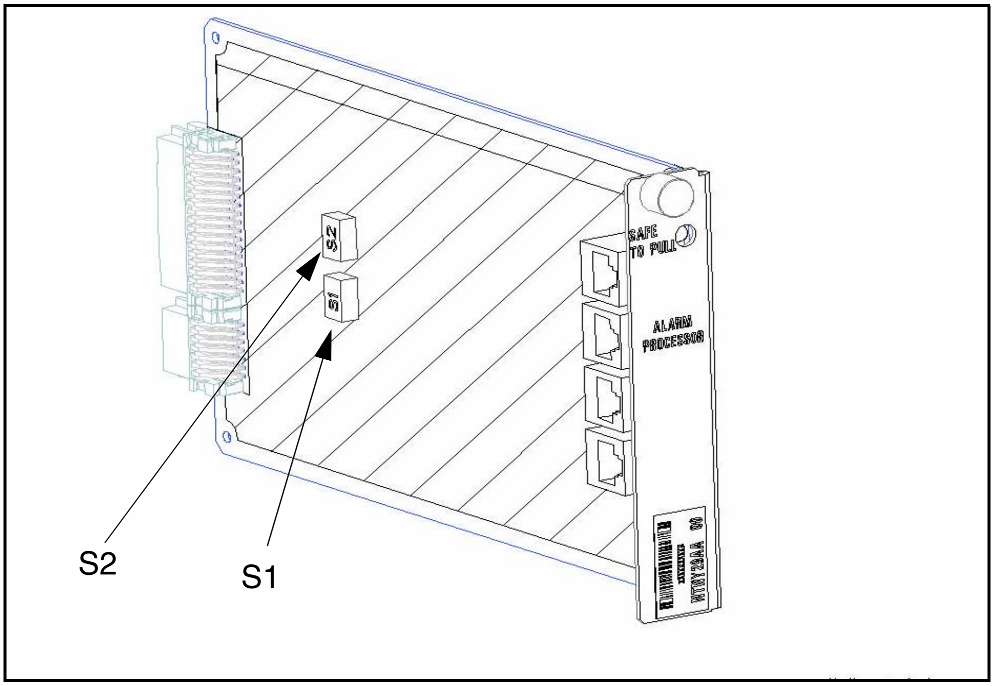
Obtain a replacement card. Verify that the replacement card has the same product equipment code (PEC), including suffix, as the card that is to be removed.

8 Remove the IBIP front cover.

9 Loosen the hold-down screw on the faceplate of the alarm processor card

10 Record the position of the two switch banks (S1 and S2) on the alarm card. Refer to the following figure for switch bank locations.

Alarm processor card switch location



11 Set the two switch banks like the card to be replaced. The following table provides settings for SW-2 used to set the power option settings.

Switch 2 Power option switch settings

SW-2 Setting				Description
1	**2**	**3**	**4**	
Off	Off	X	X	Monitor all 8 SB and TB feeds
On	Off	X	X	Monitor 2A and 2B SB and TB feeds
Off	On	X	X	Monitor 1A and 1B SB and TB feeds
On	On	X	X	No feeds monitored
X = switch setting has no impact.				

The following table provides settings for SW-1 used to set the frame id settings.

Switch 1 Frame ID switch settings

SW-1 Setting				Description
1	**2**	**3**	**4**	
Off	Off	Off	Off	Frame 0
On	Off	Off	Off	Frame 1
Off	On	Off	Off	Frame 2
On	On	Off	Off	Frame 3
Off	Off	On	Off	Frame 4
On	Off	On	Off	Frame 5
Off	On	On	Off	Frame 6
On	On	On	Off	Frame 7
Off	Off	Off	On	Frame 8
On	Off	Off	On	Frame 9
Off	On	Off	On	Frame 10

Switch 1 Frame ID switch settings

SW-1 Setting				Description
1	2	3	4	
On	On	Off	On	Frame 11
Off	Off	On	On	Frame 12
On	Off	On	On	Frame 13
Off	On	On	On	Frame 14
On	On	On	On	Frame 15

12 Insert the replacement alarm processor card into the IBIP and secure the card into place with the hold-down screw.

13 Replace the IBIP front cover.

At the MG 9000 Manager

14 To return the alarm processor card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section, wait for the Restart to complete, and set the Administrative state to Unlocked from the administrative state pull-down menu in the state section.

15 Return the card for repair or replacement according to local procedures.

16 The procedure is complete.

Replacing an NTNY30 ITP card

Purpose of this procedure

The following procedure provides the steps for replacing an Internet Telephony Processor (ITP) card which resides in slots 12 and 13 of the master shelf and of any subtending MG 9000 shelves. This procedure is typically used for an in service MG 9000 with a pair of ITP cards.

In situations where neither card has the correct load such as when a new shelf is installed or in the rare instance when both cards are faulty, the software in both cards must be upgraded. Refer to procedure “MG upgrades” in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450.

The following versions of the NTNY30 ITP card are addressed in this procedure:

- NTNY30AB - ITP card used in UA-AAL1 solution (ATM)
- NTNY30BA - ITP card used in the UA-IP solution (IP)
- NTNY30CA - ITP card used in the UA-IP solutions

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a ITP card failure or when performing an upgrade of the ITP card to an approved replacement.

> ***Note:*** If a Proxy mode fault is observed on this card, the ITP card is not communicating. It is possible the card will have a green LED lit indicating normal operation even after having been locked and offlined from the ITP Card View. This means no “Safe to pull” LED will light. Observe the alarm in the Alarm Browser and ensure the instructions for clearing this alarm in Clearing MG 9000 ITP card and VMG alarms on page 134 are followed.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an ITP card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 Double click on the shelf to access the Shelf View for the MG 9000 shelf with the ITP card to be replaced.

3 Double click on the ITP card to be replaced to access the ITP Card View.

4 Use the following table to determine the next step.

If the ITP card to be replaced is	Do
part of a card upgrade	step 5
faulty	step 6

5 Check the Standby status of the ITP card in the status section.

If this ITP card is	Do
Active and is Providing service	step 8
Idle and is in Standby status	step 9

6 Identify the ITP card with the alarm condition by observing the alarm balloon.

7 Double click on the ITP card with the alarm to access the Card View. Go to step 9.

8 To switch the activity of the currently active card to inactive, from the Actions menu at the top of the Card View, select Maintenance->Swact. A SWACT dialog box appears. In the SWACT request section, select manual warm SWACT, then click on Apply. Wait for the Standby status to change to Hot-Standby. Refer to Switching activity of a card.

9 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the state section. Refer to Locking a card.

10 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. Observe that the LED indicator on the Card View changes to red, indicating “Safe to pull.”

At the MG 9000 frame

11

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement ITP card having the same PEC and suffix as the card being replaced. If this is an approved hardware upgrade, obtain the approved replacement.

12 Carefully disconnect the ATM-25 cables on the faceplate of the ITP card. The bottom connector is for port 0. The top connector is for port 1. Carefully lay the cables aside.

13

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the ITP card in the frame, shelf, and slot number identified in the ITP Card View.

14 Carefully reconnect the ATM connectors that were disconnected in step 12.

At the MG 9000 Manager

15 Wait for the restart to complete.

16 To set the ITP card in service, at the ITP Card View set the Configuration state to Online from the configuration state pull-down menu in the State section.

17 Perform a mate load on the new card by performing the following steps:

a Select Actions->Software Upgrade from the menu bar at the top of the Card View. The Software Upgrade View appears.

b Select Actions->Load from mate from the menu bar at the top of the Software Upgrade View. Messages appear in the Upgrade status field reporting the progress of the activity.

18 Perform a restart from flash. From the Card View, select Restart Flash Primary from the pull down in the Card pane and click on Restart. Wait for the restart to complete.

Note: When restart from flash is complete, check the software attributes for the card to ensure the correct load was loaded.

19 Set the Administrative state to Unlocked from the administrative state pull-down menu in the State section.

20 Return the faulty card for repair or replacement according to local procedures.

21 This procedure is complete.

Replacing an NTNY40 DS1 card

Purpose of this procedure

The following procedure provides the steps for replacing a DS1 card which resides in the MG 9000 shelf.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a DS1 card failure.

> ***Note:*** If a Proxy mode fault is observed on this card, the DS1 card is not communicating. It is possible the card will have a green LED lit indicating normal operation even after having been locked and offlined from the DS1 Card View. This means no “Safe to pull” LED will light. Observe the alarm in the Alarm Browser. and ensure the instructions for clearing this alarm in Clearing MG 9000 DS1 card alarms on page 179 are followed.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a DS1 card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 Double click on the shelf to access the Shelf View for the MG 9000 shelf that has the faulty DS1 card.

3 Identify the DS1 card with the alarm condition by observing the alarm browser. The alarm balloon visible on the DS1 in the shelf with the fault may also show the alarm condition.

4 Double click on the DS1 card with the alarm to access the DS1 Card View.

5

> **CAUTION**
> **Loss of service**
> Multiple lines are served by the DS1 card. Replace the DS1 card during periods of low private lines traffic to reduce the impact of the loss of service.

To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the State pane. When attempting to lock a DS1 card with services, a warning message appears, informing the user that to proceed, Forced Lock must be used. Select Forced Lock and the system again presents the warning message and requests a response to the warning message to proceed.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the State pane. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

7 Perform the “Saving PLoA Services” procedure in *MG 9000 Configuration Management*, NN10096-511 to list all the services associated with the DS1 card to be replaced and return to this step.

8 Perform the “Deleting PLoA Services” procedure in *MG 9000 Configuration Management*, NN10096-511 until all affected services are deleted and return to this step.

9 At the Card View, select Services->Circuits Listing from the menu bar. Determine if any ports on the DS1 card are channelized.

The next step is based on the information in the following table.

If ports on the DS1 card	Do
are channelized	step 10
not channelized	step 12

10 Perform the “Unchannelizing ports” procedure in *MG 9000 Configuration Management*, NN10096-511 to unchannelized all channelized ports on the DS1 card and return to this procedure.

11 Perform the “Deleting DS-0 bundles on DS1 ports” procedure in *MG 9000 Configuration Management*, NN10096-511 to delete any DS-0 provisioned bundles. Repeat this procedure for all provisioned bundles on the DS1 card and return to this procedure.

At the MG 9000 frame

12

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement DS1 card having the same PEC and suffix as the card being replaced.

13 Carefully disconnect the cable from the connector on the faceplate of the DS1 card and lay the cable aside.

14

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty DS1 card in the frame, shelf, and slot number identified in the DS1 Card View screen on the Carrier VoIP MG 9000 Manager.

15 Carefully reconnect the connector(s) disconnected in step 13.

At the MG 9000 Manager

16 To return the DS1 card to service, at the DS1 Card View set the Configuration state to Online from the configuration state pull-down menu in the State pane. Set the Administrative state to Unlocked from the administrative state pull-down menu in the State section.

17 Perform the “Provisioning a DS1 card” procedure in *MG 9000 Configuration Management*, NN10096-511 to reconfigure the DS1 card to support the services that existed on the card that was replaced.

18 Perform the “Provisioning private lines services” to reprovision the private lines services that were deleted in step 8. Use the exported PLoA Services file to assist in the reprovisioning process. Return to this step.

19 Return the faulty card for repair or replacement according to local procedures.

20 This procedure is complete.

Replacing an NTNY41 ITX card

Purpose of this procedure

The following procedure identifies the steps for replacing an Internet Telephony eXtender (ITX) card which resides in the MG 9000 shelf. The following versions of the NTNY45 DCC card are addressed in this procedure:

- NTNY41AA - ITX card
- NTNY41BA - ITX card introduced in SN07

> ***Note:*** If replacing an NTNY41AA with an NTNY41BA and if the BITS interface is in use on the NTNY41AA, then the BITS connections for both cards must first be moved to the DCC card, and then proceed with installing the NTNY41BA card. Move the BITS connection to the DCC card before proceeding using the procedure provided with the NTNY41BA card. Refer to “Clock Sync Provisioning” in *MG 9000 Configuration Management*, NN10096-511 for information on setting up timing through the LCI.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating an ITX card failure.

> ***Note:*** If a Proxy mode fault is observed on this card, the ITX card is not communicating. It is possible the card will have a green LED lit indicating normal operation even after having been locked and offlined from the ITX Card View. This means no “Safe to pull” LED will light. Observe the alarm in the Alarm Browser. and ensure the instructions for clearing this alarm in Clearing MG 9000 ITX card alarms on page 125 are followed.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an ITX card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2 Double click on the shelf to access the Shelf View for the MG 9000 shelf with the faulty ITX card.

3 Double click on the ITX card to be replaced to access the ITX Card View.

4 Use the following table to determine the next step.

If the ITX card to be replaced is	Do
part of a card upgrade	step 5
faulty	step 6

5 Check the Standby status of the ITX card in the status section.

If	Do
this is the Active ITX card and indicates it is Providing Service	step 7
this ITX card is in Standby status	step 8

6 Identify the ITX card with the alarm condition by observing the alarm balloon. Go to step 8.

7 To switch the activity of the currently active card to inactive, from the Actions pull menu at the top of the Card View, select Maintenance->Swact. In the SWACT request section, select manual warm SWACT, then click on Apply. Wait for the Standby status to change to Hot-Standby. Refer to Switching activity of a card.

8 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the state section. Refer to Locking a card.

9 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. Wait for the Restart to complete. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

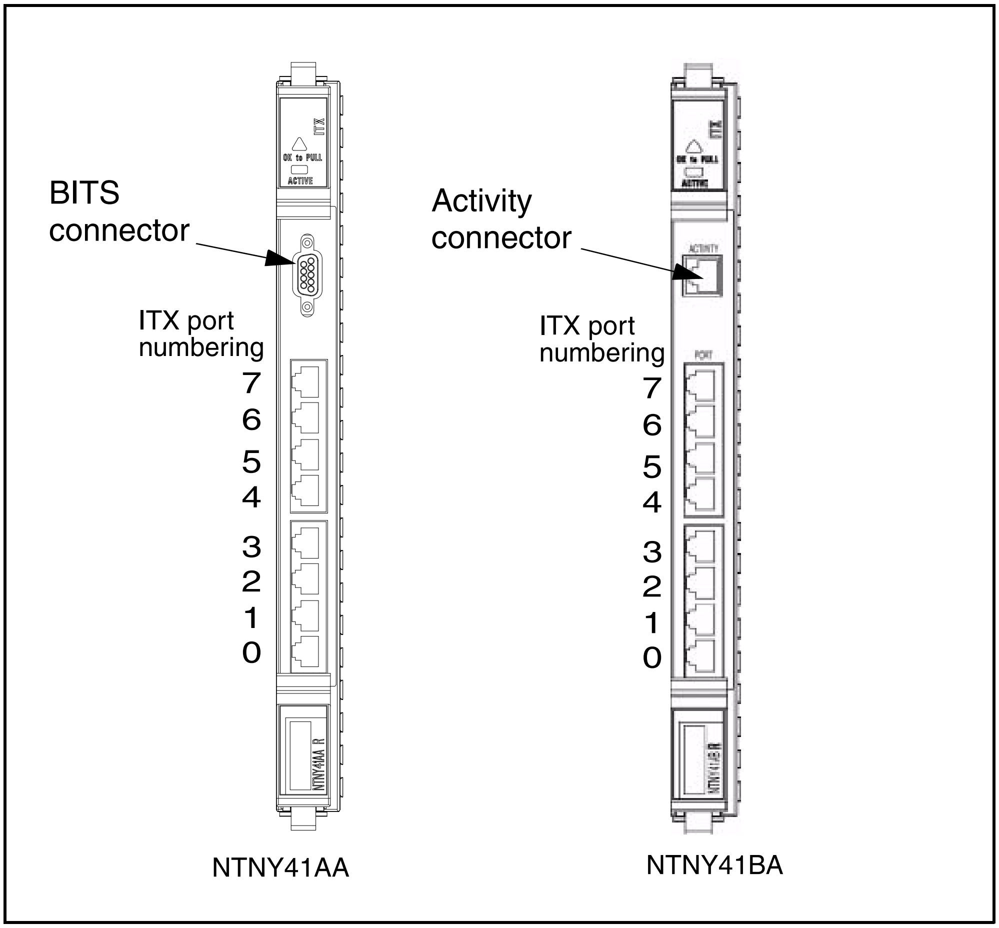
10

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement ITX card having the same PEC and suffix as the card being replaced. If this is an approved hardware upgrade obtain the approved replacement.

11 Carefully disconnect the cables from the RJ45 connectors on the faceplate of the ITX card. Label and carefully lay the cables aside. The ports are numbered as shown in the following figure. If there is a BITS cable connected to the DB9 connector on the NTNY41AA card, disconnect it. If an NTNY41BA card is being replaced, disconnect the activity cable.

ITX card port number



12

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty ITX card in the frame, shelf, and slot number identified in the Card View screen on the MG 9000 Manager.

13 Carefully reconnect the cable to the RJ45 connectors to the same ports that were disconnected in step 11. If a BITS cable was disconnected from the NTNY41AA card in step 11, reconnect the cable to the DB9 connector. Reconnect the activity cable that was disconnected from the NTNY41BA card in step 11.

At the MG 9000 Manager

14 Wait for the restart to complete.

15 To set the ITX card in service, at the ITX Card View set the Configuration state to Online from the configuration state pull-down menu in the State section.

16 Perform a mate load on the new card by performing the following steps:

- **a** Select Actions->Software Upgrade from the menu bar at the top of the Card View. The Software Upgrade View appears.
- **b** Select Actions->Load from mate from the menu bar at the top of the Software Upgrade View. Messages appear in the Upgrade status field reporting the progress of the activity.

17 Perform a restart from flash. From the Card View, select Restart Flash Primary from the pull down in the Card pane and click on Restart. Wait for the restart to complete.

> ***Note:*** When restart from flash is complete, check the software attributes for the card to ensure the correct load was loaded.

18 Set the Administrative state to Unlocked from the administrative state pull-down menu in the State section.

19 Return the faulty card for repair or replacement according to local procedures.

20 This procedure is complete.

Replacing an NTNY42 MTA-TRC card

Purpose of this procedure

The following procedure provides the steps for replacing an MTA-TRC card in the MG 9000 shelf.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a MTA-TRC card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an MTA-TRC card

At the MG 9000 Manager

1. At the Subnet View, double click the MG 9000 icon. The Frame View appears.
2. Double click on the shelf to access the Shelf View for the MG 9000 shelf with the faulty MTA-TRC card.
3. Identify the MTA-TRC card with the alarm condition by observing the alarm balloon.
4. Double click on the MTA-TRC card with the alarm to access the Card View.
5. To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu. All service will be terminated on the card. Refer to Locking a card.

   Note: If calls are in progress, the lock will fail. Attempt to lock the card later or use the Force option to drop all calls in progress.
6. Set the Configuration State to Offline from the configuration state pull-down menu in the state section. The operational state changes to “Disabled.” Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

7

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement MTA-TRC card having the same PEC and suffix as the card being replaced.

8 Carefully disconnect the connector on the faceplate of the MTA-TRC card and lay the cable aside.

9

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty MTA-TRC card in the frame, shelf, and slot number identified in the Card View screen on the MG 9000 Manager.

10 Carefully reconnect the connector that was disconnected in step 8.

At the MG 9000 Manager

11 To return the MTA-TRC card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section. Confirm the red LED is not lit.

12 Wait for the Restart to complete and set the Administrative state to Unlocked from the administrative state pull-down menu in the state section. A pop-up message appears to indicate the card has returned to service.

13 Perform a software download if the version of the software in the replacement card is older than the software version in the original card. Determine if the upgrade is necessary based on the following table.

If the software load in the replacement card is	Do
the same as the load in the replaced MTA and ITP card	step 14
incompatible with that in the replaced MTA and the ITP card	From the Card View menu bar, access the Actions->Software Download Manager. Complete the information in the Software Download Manager GUI to download the current software load into the MTA card. For more information, refer to the "Downloading software into the MTA card" procedure in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450.

14 Return the faulty card for repair or replacement according to local procedures.

15 This procedure is complete.

Replacing an NTNY43 ABI card

Purpose of this procedure

The following procedure provides the steps for replacing a DS-512 Access Bridging Interface (ABI) card in the MG 9000 shelf. The following versions of the NTNY43 card are addressed in this procedure.

- NTNY43AA - DS512 card used in the UA-AAL1 solution only
- NTNY43BA - DS512 card used in the UA-IP solutions

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm pointing to an ABI card failure or when performing an upgrade of the ABI card to an approved replacement.

> ***Note:*** If a Proxy mode fault is observed on this card, the ABI card is not communicating. It is possible the card will have a green LED lit indicating normal operation even after having been locked and offlined from the ABI Card View. This means no “Safe to pull” LED will light. Observe the alarm in the Alarm Browser. and ensure the instructions for clearing this alarm in Clearing MG 9000 DS-512 card alarms on page 185 are followed.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an ABI card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2

> **CAUTION**
> **Loss of service**
> Multiple lines are served by the XPM connected to the ABI card. In addition, both cards are part of a protection group and are providing service. Replace the ABI card during periods of low traffic to avoid loss of service.

Double click on the shelf to access the Shelf View for the MG 9000 shelf with the ABI card to be replaced.

3 Double click on the ABI card to be replaced to access the ABI Card View.

4 Use the following table to determine the next step.

If the ABI card to be replaced is	Do
part of a card upgrade	step 5
faulty	step 6

5 Determine the Service Status of the card in the ABI Card View. Use the information in the following table to determine the next step.

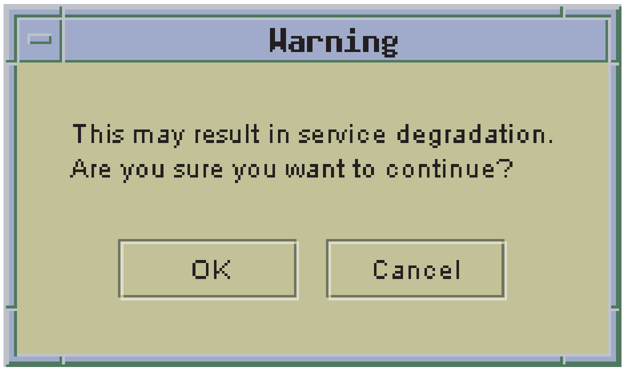
If the Service Status of the ABI card seen in the ABI Card View is	Do
Providing_Service_Master	Step 7
Providing_Service_Slave	Step 8

6 Identify the ABI card with the alarm condition by observing the alarm balloon.

7 To switch the mastership of the Master card to Slave, perform the Switching mastership of an ABI card procedure

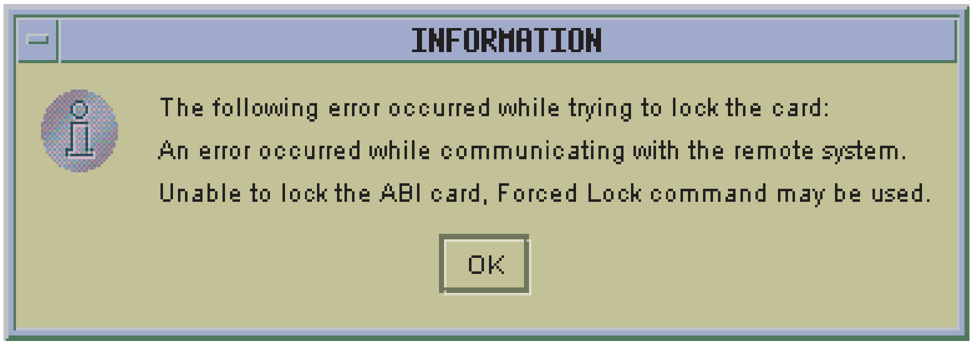
8 To lock the ABI card, change the Administrative state by selecting Lock from the administrative state pull-down menu. All service will be terminated on the card. Refer to Locking a card.

a When locking the Slave ABI card, a warning message will and an informational message will appear warning of service degradation when the Slave ABI card is taken out of service. The warning and information messages are shown next.



Warning

This may result in service degradation.
Are you sure you want to continue?



INFORMATION

The following error occurred while trying to lock the card:
An error occurred while communicating with the remote system.
Unable to lock the ABI card, Forced Lock command may be used.

To continue with locking the Slave ABI card, use the Force Lock option.

b After the lock is complete, proceed to step 9.

9 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. The operational state changes to “Disabled.” Observe that the LED indicator on the Card View changes to red, indicating “Safe to pull.”

At the MG 9000 frame

10

WARNING
Static electricity damage
Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement DS-512 card having the same PEC and suffix as the card being replaced. If this is an approved hardware upgrade, obtain the approved replacement.

11

WARNING
Risk of eye injury
At all times when handling optical fibers, follow the safety procedures recommended by your company.

Never look into an active fiber or a fiber-optic connector. Invisible light that can blind is present. Keep all optical connectors capped.

DANGER
Possible equipment damage
Make sure you do not contaminate the fiber tip surface. Do not touch the tip of the fiber. Dirt or oil from the skin transferred to the fiber tip surface degrades fiber performance.

DANGER
Damage to fiber cable.
Make sure you handle the fiber cables carefully. Do not crimp or bend the fiber cables to a radius of less than 25 mm (1 in.).

Carefully disconnect both fiber cables from the optical connectors on the faceplate of the DS-512 card. Label the cables to ensure correct replacement. The bottom connector is for the transmit (Tx) fiber and the top connector is for the receive (Rx) fiber. Carefully lay the cables aside.

12 Carefully disconnect the activity cable from the RJ45 connector on the faceplate of the DS-512 card and lay the cable aside.

13

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the ABI card in the frame, shelf, and slot number identified in the ABI Card View.

14 Carefully reconnect the activity cable to the RJ45 connector on the faceplate of the ABI card that was disconnected in step 12.

15 Carefully reconnect the fiber cables to the optical connectors on the faceplate of the ABI card that were disconnected in step 11.

At the MG 9000 Manager

16 Wait for the restart to complete.

17 To set the ABI card in service, at the ABI Card View set the Configuration state to Online from the configuration state pull-down menu in the State section.

18 Perform a mate load on the new card by performing the following steps:

a Select Actions->Software Upgrade from the menu bar at the top of the Card View. The Software Upgrade View appears.

b Select Actions->Load from mate from the menu bar at the top of the Software Upgrade View. Messages appear in the Upgrade status field reporting the progress of the activity.

19 Perform a restart from flash. From the Card View, select Restart Flash Primary from the pull down in the Card pane and click on Restart. Wait for the restart to complete.

Note: When restart from flash is complete, check the software attributes for the card to ensure the correct load was loaded.

20 Set the Administrative state to Unlocked from the administrative state pull-down menu in the State section.

21 Return the faulty card for repair or replacement according to local procedures.

22 This procedure is complete.

Replacing an NTNY45 DCC card

Purpose of this procedure

The following procedure identifies the steps for replacing an NTNY45 Data Control Card (DCC) in slots 10 and 11 of the master MG 9000 shelf. The following versions of the NTNY45 DCC card are addressed in this procedure:

- NTNY45AA - Data control card with OC-3c WAN
- NTNY45BA - Data control card with 8 port IMA WAN
- NTNY45CA - Data control card with OC-3/STM-1
- NTNY45FA - Data control card with Gigabit Ethernet (GigE)

> ***Note:*** In this procedure, the DCC is also known as the OC-3 card, and is also known as OC-3 in many of the GUI screens. When the DCC is a DS1 IMA card, the GUI screen will label the DCC accordingly.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a DCC card failure or when performing an upgrade of the DCC card to an approved replacement.

> ***Note:*** If a Proxy mode fault is observed on this card, the DCC card is not communicating. It is possible the card will have a green LED lit indicating normal operation even after having been locked and offlined from the DCC Card View. This means no “Safe to pull” LED will light. Observe the alarm in the Alarm Browser. and ensure the instructions for clearing this alarm in Clearing MG 9000 DCC card alarms on page 102 are followed.

Prerequisites

Remote LCI

Remote LCI provides the ability to connect directly to the DCC card using IP and a web browser such as Internet Explorer or Netscape without having to connect a laptop PC physically into the LCI port on the faceplate of the card. Perform the following steps before attempting to replace a DCC card:

1. Attempt to connect to the active DCC card's IP address. using a web browser by typing the following in the URL field:

   ```
   https://xxx.xxx.xxx.xx:443
   ```

   where

   xxx.xxx.xxx.xx is a customer provisioned, site-specific IP address for connecting to the DCC using Remote LCI

   The system responds with a request for user id and password

   Note: If this step is successful proceed to step 2. If unsuccessful, Remote LCI is not used. Proceed to the card replacement procedure.

2. In the LCI, click on the Maintenance button at the top right of the screen to open the Maintenance screen.
3. In Select a shelf view, scroll through the list of shelves and select the shelf containing the DCC card to be replaced.
4. Click on the DCC card to be replaced.
5. Click on Ethernet Config from the menu on the left.
6. Click on Query and record the following values:
   - IP address
   - Subnet Mask
   - Default Gateway
7. Have these values available for entry after the DCC card is replaced.

Action

Replacing a DCC card

At the MG 9000 Manager

1 Determine if Remote LCI is used to communicate with the DCC card being replaced. Go to Prerequisites on page 406 in this procedure before proceeding. If Remote LCI is not used, go to step 2.

2 At the Subnet View, double click the MG 9000 icon. The Desktop NE view containing the Frame View appears.

3 Double click on the shelf to access the Shelf View for the MG 9000 shelf that has the DCC card to be replaced.

4 If the DCC card is in fault, identify the DCC card with the alarm condition by observing the alarm balloon.

5 Double click on the DCC card with the alarm to access the Card View.

6 Check the Standby status of the DCC in the status section.

If	Do
this is the Active DCC card and indicates it is Providing Service	step 7
this DCC card is in Hot-standby status	step 8

7 To switch the activity of the currently active card to inactive, from the Actions menu at the top of the Card View, select Maintenance->Swact. A SWACT dialog box appears. In the SWACT request section, select manual warm SWACT, then click on Apply. Wait for the Standby status to change to Hot-Standby. Refer to Switching activity of a card.

8 To lock the card, change the Administrative state by selecting Locked from the administrative state pull-down menu in the state section. Refer to Locking a card.

9 The next step depends on the information in the following table.

If the DCC card being replaced is	Do
an NTNY45AA/CA with OC-3 connectors on the faceplate	step 10
an NTNY45BA with a DS1 IMA connector on the faceplate	step 14
an NTNY45FA with an NTTP62 SFP tranceiver device connected to a GigE connector on the faceplate	step 13

10 Use the information in the following table to determine the next step.

If the OC3 carrier	Do
is channelized	step 11
is concatenated	step 12

11 At the Card View, double click on the OC3 Port icon. The STS1 port view appears showing the network carrier path. Perform the following to lock the STS1 path in the carrier.Double-click on the

path icon, the STS1 Path tab comes to the foreground. Select Locked from the Administrative status pull down menu to set the path to Locked. Click on the OC3 Attributes tab and select Locked from the Administrative status pull down menu. Refer to Locking an OC3/STS1 carrier path.

12 To disable the OC-3 laser, at the Card View select the OC-3 port by double-clicking on the port icon. The OC-3 Port View appears. Select Lock from the Administrative status pull-down menu. Select Off line from the Configuration status pull-down menu. Go to step 14.

13 At the Card View, double click on the GigE Port 0 icon. The GigE port view appears. Perform the following to lock the GigE link. Click on the Link Controls tab. Select Locked from the Administrative status pull down menu to set the link to Locked. Refer to Locking a GigE port and link on page 364.

14 At the DCC Card View, set the Configuration State to Offline from the configuration state pull-down menu in the state section. Observe that the LED indicator on the Card View changes to red, indicating “Safe to pull.”

At the MG 9000 frame

15

WARNING
Static electricity damage
Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement DCC card having the same PEC and suffix as the card being replaced.

16

WARNING
Equipment damage
Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

The next step depends on the information in the following table.

If the DCC card being replaced is	Do
an NTNY45AA/CA with OC-3 connectors on the faceplate	step 17
an NTNY45BA with a DS1 IMA connector on the faceplate	step 18
an NTNY45FA with a GigE connector on the faceplate	step 19

17

WARNING

Risk of eye injury

At all times when handling optical fibers, follow the safety procedures recommended by your company.

Never look into an active fiber or a fiber-optic connector. Invisible light that can blind is present. Keep all optical connectors capped.

DANGER

Possible equipment damage

Make sure you do not contaminate the fiber tip surface. Do not touch the tip of the fiber. Dirt or oil from the skin transferred to the fiber tip surface degrades fiber performance.

DANGER

Damage to fiber cable.

Make sure you handle the fiber cables carefully. Do not crimp or bend the fiber cables to a radius of less than 25 mm (1 in.).

Gently withdraw, but do not remove the card from the slot, to disconnect the card from the backplane connector. Carefully disconnect both OC3 fiber cables from the optical connectors on the faceplate of the DCC card. Label the cables to ensure correct replacement. The bottom connector is for the transmit (Tx) fiber and the top connector is for the receive (Rx) fiber. Disconnect the BITS cable (optional). Go to step 20.

18 Carefully disconnect the DS1IMA Y-cable and the BITS cable (optional) on the faceplate of the DCC card. Go to step 20.

19 Carefully disconnect the GigE fiber cable from the NTTP62 small-form factor pluggable (SFP) transciever device. Then using the latch, pull to withdraw the SFP from the faceplate of the GigE DCC card. Disconnect the BITS cable.

20 Remove and replace the faulty DCC card in the frame, shelf, and slot number identified in the Card View on the MG 9000 Manager.

21 Carefully reconnect the cables that were disconnected in step 17 or 18 to their original positions. For the GigE card, insert the NTTP62 SFP into the same GigE port from which the SFP was removed in step 19 and connect the fiber cable to the SFP.

At the MG 9000 Manager

22 Use the information in the following table to determine the next step.

If the DCC card replaced is	Do
an NTNY45AA/CA with OC-3 connectors on the faceplate	step 23
an NTNY45BA with a DS1 IMA connector on the faceplate	step 29
an NTNY45FA with a GigE connector on the faceplate	step 23

23 Wait for the restart of the DCC card to complete.

24 Use the information in the following table to determine the next step.

If the DCC card replaced is	Do
an NTNY45AA/CA with OC-3 connectors on the faceplate	step 25
an NTNY45BA with a DS1 IMA connector on the faceplate	step 29
an NTNY45FA with a GigE connector on the faceplate	step 28

25 After the restart completes, enable the OC-3 laser. To enable the OC-3 laser, at the OC-3 Port View select Online from the Configuration status pull-down menu. Select Unlocked from the Admin status pull-down menu.

26 Use the information in the following table to determine the next step.

If the OC3 carrier	Do
is channelized	step 27
is concatenated	step 29

27 At the Card View, unlock the STS1 path in the carrier that was locked in step 11 by double-clicking on the path icon. The STS1 Path tab comes to the foreground. Click on the OC3 Attributes tab and select Unlocked from the Administrative status pull down menu. Click on the STS1 Path tab and select Unlocked from the Administrative status pull down menu to unlock the path. Refer to Unlocking an OC3/STS1 carrier path on page 361. Go to step 29.

28 At the Card View, unlock the GigE port 0 that was locked in step13 by double-clicking on the GigE Port 0 icon. The GigE port view appears. Click on the Link Controls tab and select Unlocked from the Administrative status pull down menu. Refer to Unlocking a GigE port and link on page 365.

29 Perform a mate load on the new card by performing the following steps:

a Select Actions->Software Upgrade from the menu bar at the top of the Card View. The Software Upgrade View appears.

b To set the DCC card in service, at the DCC Card View, set the Configuration state to Online from the configuration state pull-down menu in the State section.

c Select Actions->Load from mate from the menu bar at the top of the Software Upgrade View. Messages appear in the Upgrade status field reporting the progress of the activity.

30 Perform a restart from flash. From the Card View, select Restart Flash Primary from the pull down in the Card pane and click on Restart. Wait for the restart to complete.

Note: When restart from flash is complete, check the software attributes for the card to ensure the correct load was loaded.

31 Set the Administrative state to Unlocked from the administrative state pull-down menu in the State section. Verify all alarms for this card are cleared.

32 Use the information in the following table to determine the next step.

If the DCC card that was replaced	Do
connects to Remote LCI	step 33
does not connect to Remote LCI	step 34

33 Using the information that was recorded from the steps performed in Prerequisites on page 406, perform the following steps to enter the values for Remote LCI to match those in the mate card.

a Access the active DCC card of the MG 9000 network element using Remote LCI.

b In the LCI, click on the Maintenance button at the top right of the screen to open the Maintenance screen.

c In Select a shelf view, scroll through the list of shelves and select the shelf containing the DCC card that was replaced.

d Click on the DCC card that was replaced.

e Click on Ethernet Config from the menu on the left.

f Change the values to match those that were recorded from the old card and click on Submit.

34 Return the faulty card for repair or replacement according to local procedures.

35 This procedure is complete.

Replacing an NTTP62 SFP transceiver device

Purpose of this procedure

Use this procedure to replace an NTTP62 small form factor pluggable (SFP) transceiver device that plugs into each GigE port of an NTNY45FA GigE DCC card. The following versions of the NTTP62 SFP transceiver device are addressed in this procedure:

- NTNY62AF - SFP SX transceiver device (future)
- NTTP62CA - SFP LX transceiver device

When to use this procedure

Perform this procedure when it is necessary to replace a faulty SFP device on the faceplace of an NTNY45FA GigE DCC card. The SFP is reported as faulty by GIGE alarms reported to the Alarm Browser.

Action

Replacing an NTTP62 SFP transceiver device

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Desktop NE view containing the Frame View appears.

2 Double click on the shelf to access the Shelf View for the MG 9000 shelf that has the GigE DCC card with the SFP device to be replaced.

3 Identify the GigE DCC card with the faulty SFP device based on the alarm condition by observing the alarm balloon.

4 Double click on the GigE DCC card with the alarm to access the Card View.

5 Check the Standby status of the GigE DCC in the status section.

If	Do
this is the Active GigE DCC card and indicates it is Providing Service	step 6
this GigE DCC card is in Hot-standby status	step 7

6 To switch the activity of the currently active card to inactive, from the Actions menu at the top of the Card View, select Maintenance->Swact. A SWACT dialog box appears. In the SWACT request section, select manual warm SWACT, then click

on Apply. Wait for the Standby status to change to Hot-Standby. Refer to Switching activity of a card on page 343.

7 At the Card View, double click on the GigE Port 0 icon. The GigE port view appears. Perform the following to lock the GigE link. Click on the Link Controls tab. Select Locked from the Administrative status pull down menu to set the link to Locked. Refer to Locking a GigE port and link on page 364.

At the MG 9000 frame

8

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement SFP transceiver device having the same PEC and suffix as the SFP device being replaced.

9

> **WARNING**
> **Risk of eye injury**
> At all times when handling optical fibers, follow the safety procedures recommended by your company.
>
> Never look into an active fiber or a fiber-optic connector. Invisible light that can blind is present. Keep all optical connectors capped.

> **DANGER**
> **Possible equipment damage**
> Make sure you do not contaminate the fiber tip surface. Do not touch the tip of the fiber. Dirt or oil from the skin transferred to the fiber tip surface degrades fiber performance.

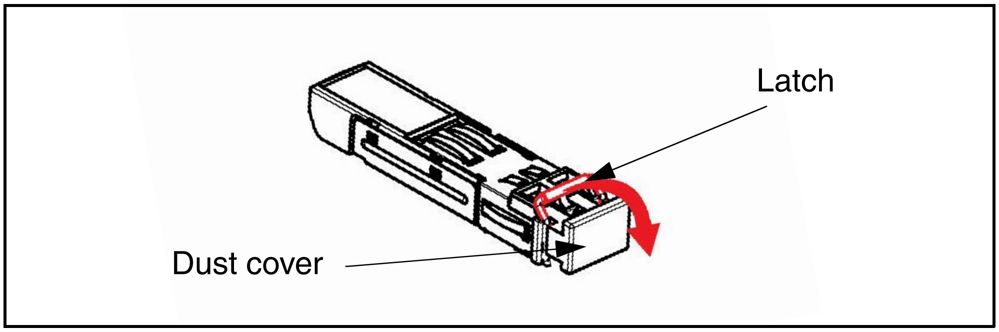
DANGER

Damage to fiber cable.

Make sure you handle the fiber cables carefully. Do not crimp or bend the fiber cables to a radius of less than 25 mm (1 in.).

Carefully disconnect the GigE fiber cable from the NTTP62 SFP transceiver device. Then using the latch, pull to withdraw the SFP from the faceplate of the GigE DCC card.

NTTP62 SFP transceiver device



10 Insert the replacement SFP device into the same GigE port from which the faulty SFP was removed and ensure it is seated. Remove the dust cover. Carefully connect the GigE fiber cable into the SFP device.

At the MG 9000 Manager

11 At the Card View, unlock the GigE port 0 that was locked in step 7 by double-clicking on the GigE Port 0 icon. The GigE port view appears. Click on the Link Controls tab and select Unlocked from the Administrative status pull down menu. Refer to Unlocking a GigE port and link on page 365.

12 This procedure is complete.

Replacing an NTNY50 POTS32 card

Purpose of this procedure

The following procedure provides the steps for replacing an NTNY50 POTS32 line card which resides in the MG 9000 shelf. The term POTS32 refers to the World line card (WLC). The term WLC is used to correspond with the screen title.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a POTS 32 card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a POTS32 line card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2

> **CAUTION**
> **Loss of service**
> Multiple lines are served by the POTS32 card. Replace the POTS32 card during periods of low traffic to avoid loss of service.

Double click on the shelf to access the Shelf View for the MG 9000 shelf with the faulty POTS32 line card.

3 Identify the POTS32 line card with the alarm condition by observing the alarm balloon.

4 Double click on the POTS 32 card with the alarm to access the Card View.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu. All service will be terminated on the card. Refer to Locking a card.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. The operational state changes to Disabled. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

7

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement POTS32 line card having the same PEC and suffix as the card being replaced.

8 Carefully disconnect the connector on the faceplate of the POTS32 line card. Carefully lay the cable aside.

9

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty POTS32 line card in the frame, shelf, and slot number identified in the Card View screen on the MG 9000 Manager.

10 Carefully reconnect the connector that was disconnected in step 8.

At the MG 9000 Manager

11 To return the POTS32 line card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section. Confirm the red LED is not lit.

12 Set the Administrative state to unlocked from the Administrative state pull-down menu in the State section.

13 Return the faulty card for repair or replacement according to local procedures.

14 This procedure is complete.

Replacing an NTNY51 SAA card

Purpose of this procedure

The following procedure provides the steps for replacing an SAA card in the MG 9000 shelf.

> ***Note:*** The SAA card is not used in the UA-IP solution.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a SAA card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an SAA card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2

> **CAUTION**
> **Loss of service**
> Multiple lines are served by the SAA card. Replace the SAA card during periods of low traffic to avoid loss of service.

Double click on the shelf to access the Shelf View for the MG 9000 shelf with the faulty SAA card.

3 Identify the SAA card with the alarm condition by observing the alarm balloon.

4 Double click on the SAA card with the alarm to access the Card View.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu. All service will be terminated on the card. Refer to Locking a card.

> ***Note:*** If calls are in progress, the lock will fail. Attempt to lock the card later or use the Force option to drop all calls in progress.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. The operational state changes to Disabled. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

7

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement SAA card having the same PEC and suffix as the card being replaced.

8 Carefully disconnect the connector on the faceplate of the SAA card and lay the cable aside.

9

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty SAA card in the frame, shelf, and slot number identified in the Card View screen on the MG 9000 Manager.

10 Carefully reconnect the connector that was disconnected in step 8.

At the MG 9000 Manager

11 To return the SAA card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section. Confirm the red LED is not lit.

12 Set the Administrative state to unlocked from the Administrative state pull-down menu in the State section.

13 Return the faulty card for repair or replacement according to local procedures.

14 This procedure is complete.

Replacing an NTNY52 ADSL 8+8 card

Purpose of this procedure

The following procedure provides the steps for replacing an ADSL 8+8 card which resides in the MG 9000 shelf. The term ADSL signifies a specific type of DSL card, in this case asynchronous DSL. XDSL is used to correspond with the screen title, where the “X” represents a variable to include multiple Digital Subscriber Loop versions.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a ADSL 8+8 card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an ADSL 8+8 line card

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2

> **CAUTION**
> **Loss of service**
> Multiple lines are served by the ADSL card. Replace the ADSL card during periods of low traffic to avoid loss of service.

Double click on the shelf to access the Shelf View for the MG 9000 shelf with the faulty ADSL 8+8 line card.

3 Identify the ADSL 8+8 line card with the alarm condition by observing the alarm balloon.

4 Double click on the ADSL 8+8 line card with the alarm to access the Card View.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu. All service will be terminated on the card. Refer to Locking a card.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. The operational state

changes to “Disabled.” Observe that the LED indicator on the Card View changes to red, indicating “Safe to pull.”

At the MG 9000 frame

7

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement ADSL 8+8 line card having the same PEC and suffix as the card being replaced.

8 Carefully disconnect the connector on the faceplate of the ADSL 8+8 line card. Carefully lay the cable aside.

9

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty ADSL 8+8 line card in the frame, shelf, and slot number identified in the Card View screen on the MG 9000 Manager.

10 Carefully reconnect the connector that was disconnected in step 8.

At the MG 9000 Manager

11 To return the ADSL 8+8 line card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section. Confirm the red LED is not lit.

12 Set the Administrative state to Unlocked from the administrative state pull-down menu in the state section. A pop-up message appears to indicate that a restart has completed and the card has returned to service.

13 Perform a software download if the version in the replacement card is older than the software version in the original card. Determine if the software download is necessary based on the following table.

If the software load in the replacement card is	Do
the same as the load in the replaced ADSL card	step 14
incompatible with that in the replaced ADSL card	From the Card View menu bar, access the Actions->Software Download Manager. Complete the information in the Software Download Manager GUI to download the current software load into the ADSL card. For more information, refer to the “Downloading software into the xDSL card” procedure in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450

14 Return the faulty card for repair or replacement according to local procedures.

15 This procedure is complete.

Replacing an NTNY53 GLC card

Purpose of this procedure

Use this procedure to replace the following NTNY53 cards that reside in the MG 9000 shelf:

- NTNY53AA 32-line Global Line Card (GLC)
- NTNY53BA (32-line GLC)
- NTNY53CA (12-line GLC)

Note: The NTNY53BA GLC can safely replace the GLC NTNY53AA and the WLC 32 without deprovisioning prior to replacement. The NTNY53CA 12-line GLC can only safely replace the SAA-12 card without deprovisioning prior to replacement.

When to use this procedure

Use this procedure when the MG 9000 Manager indicates an alarm indicating a GLC card failure.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a GLC

At the MG 9000 Manager

1 At the Subnet View, double click the MG 9000 icon. The Frame View appears.

2

> **CAUTION**
> **Loss of service**
> Multiple lines are served by GLC cards. Replace the card during periods of low traffic to avoid loss of service.

Double click on the shelf to access the Shelf View for the MG 9000 shelf with the faulty GLC line card.

3 Identify the GLC line card with the alarm condition by observing the alarm balloon.

4 Double click on the GLC card with the alarm to access the GLC Card View.

5 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu. All service will be terminated on the card. Refer to Locking a card.

6 Set the Configuration State to Offline from the configuration state pull-down menu in the state section. The operational state changes to Disabled. Observe that the LED indicator on the Card View changes to red, indicating Safe to pull.

At the MG 9000 frame

7

> **WARNING**
> **Static electricity damage**
> Wear a wrist strap that connects to the wrist-strap grounding point to handle cards. The wrist-strap grounding point is on the local craft access panel (LCAP). The wrist strap protects the cards against static electricity damage.

Get a replacement GLC line card having the same PEC and suffix as the card being replaced.

8 Carefully disconnect the connector on the faceplate of the GLC line card. Carefully lay the cable aside.

9

> **WARNING**
> **Equipment damage**
> Ensure the red “Safe to pull” LED is lit before pulling the card. Damage to the card can result from removing the card when in the incorrect state.

Replace the faulty GLC line card in the frame, shelf, and slot number identified in the GLC Card View on the MG 9000 Manager.

10 Carefully reconnect the connector that was disconnected in step 8.

At the MG 9000 Manager

11 To return the GLC line card to service, set the Configuration state to Online from the configuration state pull-down menu in the state section. Confirm the red LED is not lit.

12 Set the Administrative state to unlocked from the Administrative state pull-down menu in the State section.

13 Return the faulty card for repair or replacement according to local procedures.

14 This procedure is complete.

Replacing a fuse in the IBIP

Purpose of this procedure

Use the following procedure to replace the fuses in the NTNY17BA intelligent bay interface panel (IBIP) identified in the table that follows.

Part number	Name
A0108989	1 Amp ABS cricket fuse
A0898425	12 Amp plug-in fuse module
A0898426	15 Amp plug-in fuse module

When to use this procedure

Use this procedure when a fuse fails in the IBIP.

Prerequisites

This procedure has no prerequisites.

Action

Replacing a fuse in an IBIP

At your current location

1 Proceed only if you have been directed to this replacement procedure by your maintenance support group.

2 Obtain a replacement fuse. Verify that the replacement fuse has the same current rating, product equipment code (PEC), including suffix, as the fuse to be removed.

At the MG 9000 frame

3 If replacing a talk battery or signal battery fuse, make sure the MG 9000 shelf components are redundantly powered from the PDC feeds.

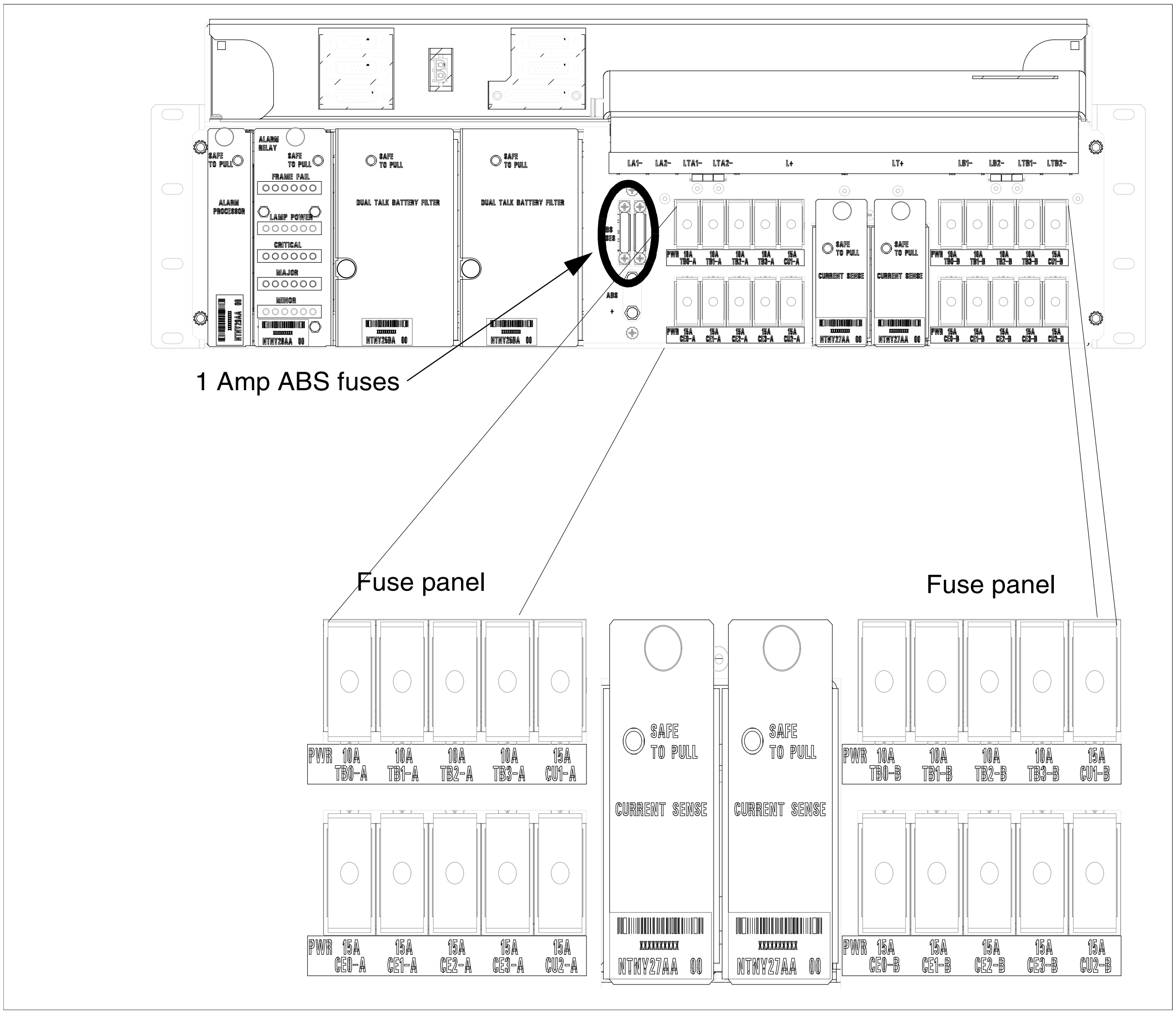
The following table lists the fuses on the faceplate of the IBIP.

Fuse label	Description	Fuse rating
ABS fuse	ABS fuse (left) - power to alarm lamps on front of NTNY28AA	1 A
ABS fuse	ABS fuse (right) - power to end aisle lamp and ABS test jacks	1 A
TB0-A	Talk battery A feed to shelf 0	12 A
TB0-B	Talk battery B feed to shelf 0	12 A
TB1-A	Talk battery A feed to shelf 1	12 A
TB1-B	Talk battery B feed to shelf 1	12 A
TB2-A	Talk battery A feed to shelf 2	12 A
TB2-B	Talk battery B feed to shelf 2	12 A
TB3-A	Talk battery A feed to shelf 3	12 A
TB3-B	Talk battery B feed to shelf 3	12 A
CU0-A	Cooling unit 0 talk battery A feed (bottom)	15 A
CU0-B	Cooling unit 0 talk battery B feed (bottom)	15 A
CU1-A	Cooling unit 1 talk battery A feed (top)	15 A
CU1-B	Cooling unit 1 talk battery B feed (top)	15 A
CE0-A	Signal battery A feed to shelf 0	15 A
CE0-A	Signal battery B feed to shelf 0	15 A
CE1-A	Signal battery A feed to shelf 1	15 A
CE1-A	Signal battery B feed to shelf 1	15 A
CE2-A	Signal battery A feed to shelf 2	15 A
CE2-A	Signal battery B feed to shelf 2	15 A

Fuse label	Description	Fuse rating
CE3-A	Signal battery A feed to shelf 3	15 A
CE3-A	Signal battery B feed to shelf 3	15 A

The following figure shows the IBIP and fuse location.

IBIP panel showing the fuse panel and ABS fuses



Note: This procedure can be performed on equipment in service without the need to power down the shelves. However, it is recommended that this procedure be performed during periods of low traffic.

4 Remove the IBIP front cover by pulling it towards you.

5. Pull out the fuse with the blown fuse indicator.
6. To ensure pin alignment, insert the replacement fuse into the empty slot with care.
7. Replace the IBIP cover.
8. Verify that the alarm clears.
9. The procedure is complete.

Replacing an air filter element

Purpose of this procedure

Use this procedure to change the air filter element in an NTNY15AA air filter unit in a MG 9000 frame.

When to use this procedure

Use this procedure it is necessary to change the air filter element according to local procedures.

Prerequisites

This procedure has no prerequisites.

Action

Replacing an air filter element

At the MG 9000 frame

1 Disengage the air filter from its locking mechanism by quickly pushing and releasing the front face of the air filter unit.

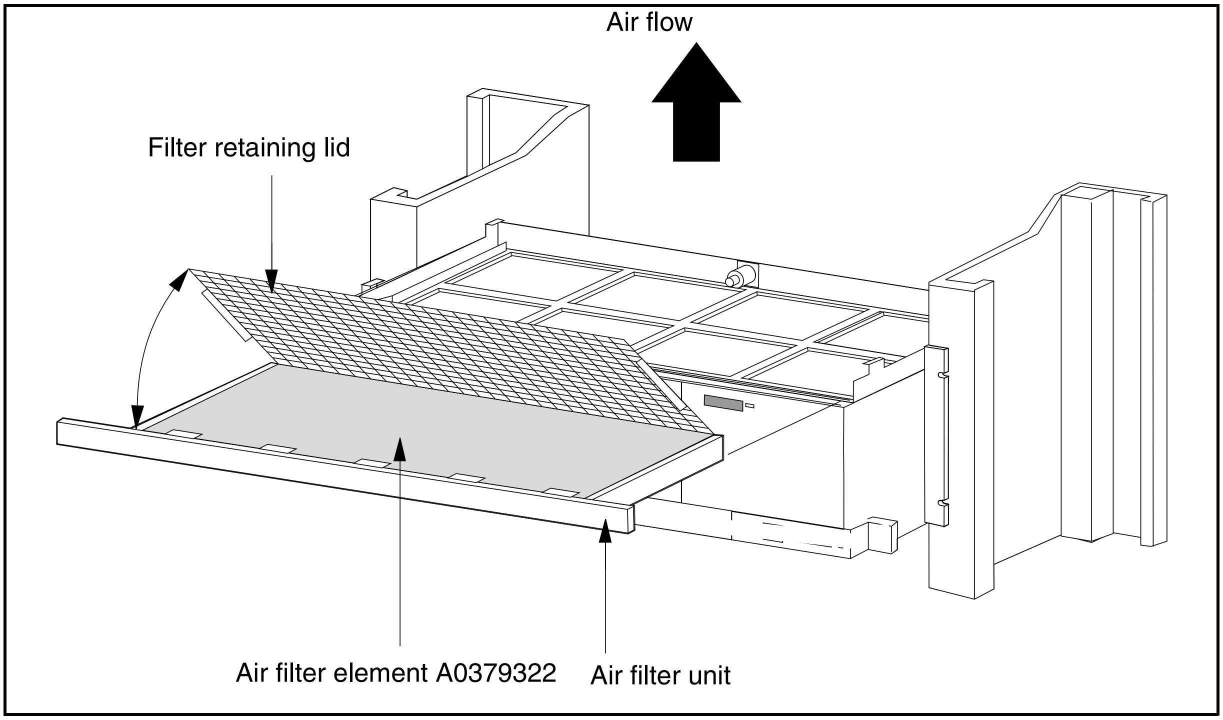
2 Withdraw the air filter by pulling it outwards.

3 Lift the filter retaining lid, remove the old filter element and replace it with a new filter element (Nortel part number A0379322).

> ***Note:*** Make sure the new air filter element is positioned correctly for the air flow (in accordance with filter manufacturers' instructions).

4 Close the filter retaining lid, and reinsert the air filter unit into the shelf until it locks into place. Refer to the following figure that shows the filter element in the air filter unit.

Air filter unit and element



5 This procedure is complete.

Outside plant cabinet procedures

Use the procedures in this section to clear faults and perform routine maintenance activities related to the outside plant cabinet (OPC).

The following are fault clearing procedures for components in the outside plant cabinet:

- Replacing batteries in OPC on page 436
- Replacing a dc power system module in OPC on page 439
- Replacing a lightning protector module in OPC on page 441
- Replacing a fuse in OPC on page 444
- Replacing the NTM906MA fan tray in the OPC on page 446
- Replacing a surge protector in the OPC on page 448
- Replacing a heat exchanger blower in the MG 9000 OPC on page 451

The following are routine maintenance procedures to be used to maintain the outside plant cabinet:

- Removing dust from OPC on page 460
- Cleaning and testing fans in OPC on page 461
- Inspecting and cleaning batteries in OPC on page 463
- Performing a GFCI check in OPC on page 466
- Performing a ground check in OPC on page 467
- Wrist strap grounding cords test on page 470

Replacing batteries in the MG 9000 OPC

Purpose of this procedure

Use this procedure to replace batteries in an MG 9000 outside plant cabinet.

When to use this procedure

Perform this procedure when it is necessary to replace batteries in an MG 9000 outside plant cabinet.

Action

Replacing batteries in OPC

At the MG 9000 outside plant cabinet site

1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front access door.

2 Use a T25 Torx driver to remove the three Torx screws and open the rear battery access door.

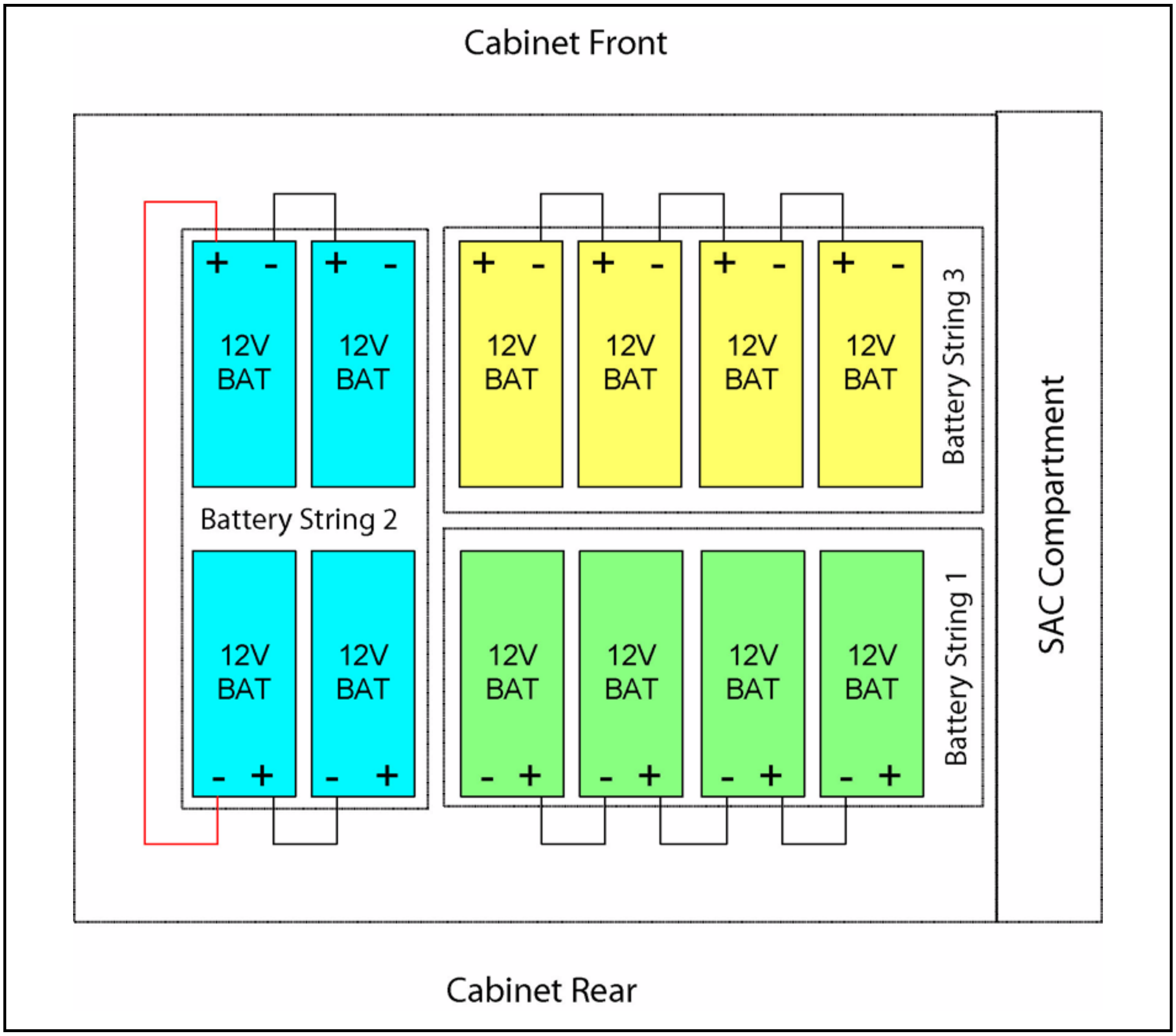
3

> **DANGER**
> **Hazardous chemicals**
> Battery chemical can be dangerous and potentially explosive. Exercise caution.

Inspect battery packs, connections, and floor for moisture or corrosion.

4 Identify the affected string(s) to be replaced. Use the following figure to identify the battery strings.

Battery arrangement in the outside plant cabinet



5

CAUTION

Possible loss of service during battery replacement.

Do not disconnect more than one battery string at a time. If more than one battery string is turned off at a time and ac power is interrupted, service may be interrupted.

Open the service access compartment (SAC) door and set the affected battery string breaker on the battery disconnect panel to Off. The battery disconnect panel is located at the top right corner of the SAC compartment.

6 In the battery compartment, disconnect and remove the affected battery string from the affected area.

7 Replace the entire battery string and connect the new battery string.

8 In the SAC compartment, set the breaker for the de-energized battery string to the On position.

9 Close the battery compartment access door and use the T25 Torx driver to tighten the three Torx screws.

10 Close the front cabinet and SAC doors. Use the 3/8 in nut driver to latch the doors. Lock the doors.

11 This procedure is complete.

Replacing a dc power system module in the MG 9000 OPC

Purpose of this procedure

Use this procedure to replace a dc power system module in the MG 9000 outside plant cabinet. Specific information on the rectifier shelf is provided in *Tyco Electronics Yukon Power Systems -48 V Indoor/Outdoor Battery Plant Product Manual*, Select Code 167-102-103.

When to use this procedure

Perform this procedure as needed. A faulty rectifier module is identified by observing the LEDs on the face of the modules. Refer to *Tyco Electronics Yukon Power Systems -48 V Indoor/Outdoor Battery Plant Product Manual*, Select Code 167-102-103 for troubleshooting information.The Yukon Power System manual provides the information needed to determine if intervention is needed in an alarm condition and if it is necessary to replace a rectifier module or control module card. This procedure is to be used only after it has been determined that a rectifier module or control module card must be replaced.

Action

Replacing a dc power system module in OPC

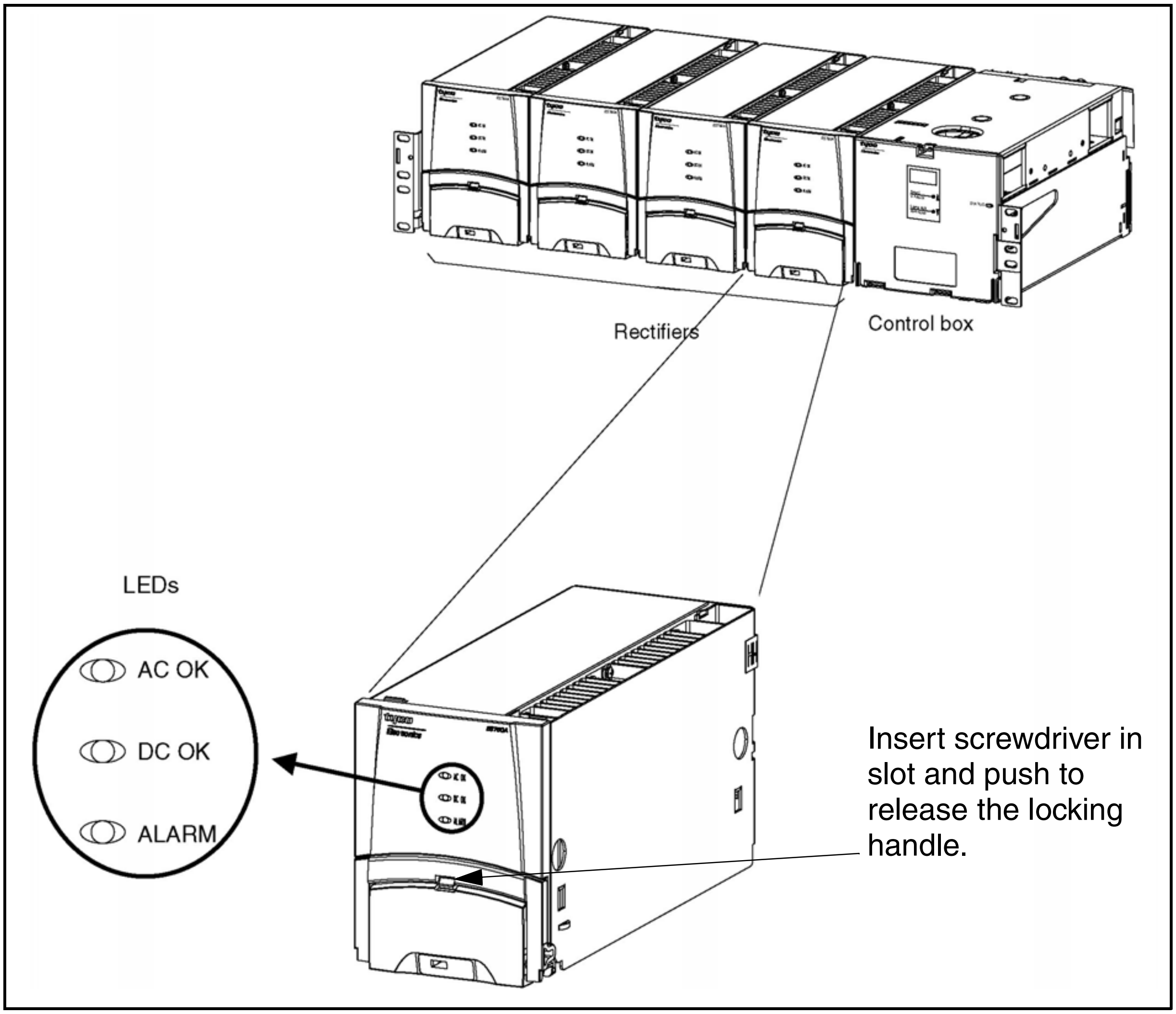
At the MG 9000 outside plant cabinet

1 Obtain a replacement module or card.

2 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front access door.

3 Identify the faulty component by noting the LEDs on the faceplate. Refer to *Tyco Electronics Yukon Power Systems -48 V Indoor/Outdoor Battery Plant Product Manual*, Select Code 167-102-103 for information on identifying the faulty component, troubleshooting, and component replacement activities.

The following figure shows the rectifier shelf, the handle release slot, and alarm LEDs.


Rectifiers
Control box
LEDs
AC OK
DC OK
ALARM
Insert screwdriver in slot and push to release the locking handle.

4 Close and use a 3/8 in. nut driver to turn the door latch on the front access compartment door. Lock the door.

5 Return the faulty module to Nortel Networks for repair according to local policy.

6 This procedure is complete.

Replacing a lightning protector module in the MG 9000 OPC

Purpose of this procedure

Use this procedure to replace a lightning protector module in the MG 9000 outside plant cabinet (OPC).

When to use this procedure

Perform this procedure as needed. A faulty lightning protector module is noted by a loss of service on an individual line.

Action

Replacing a lightning protector module in OPC

At the MG 9000 outside plant cabinet

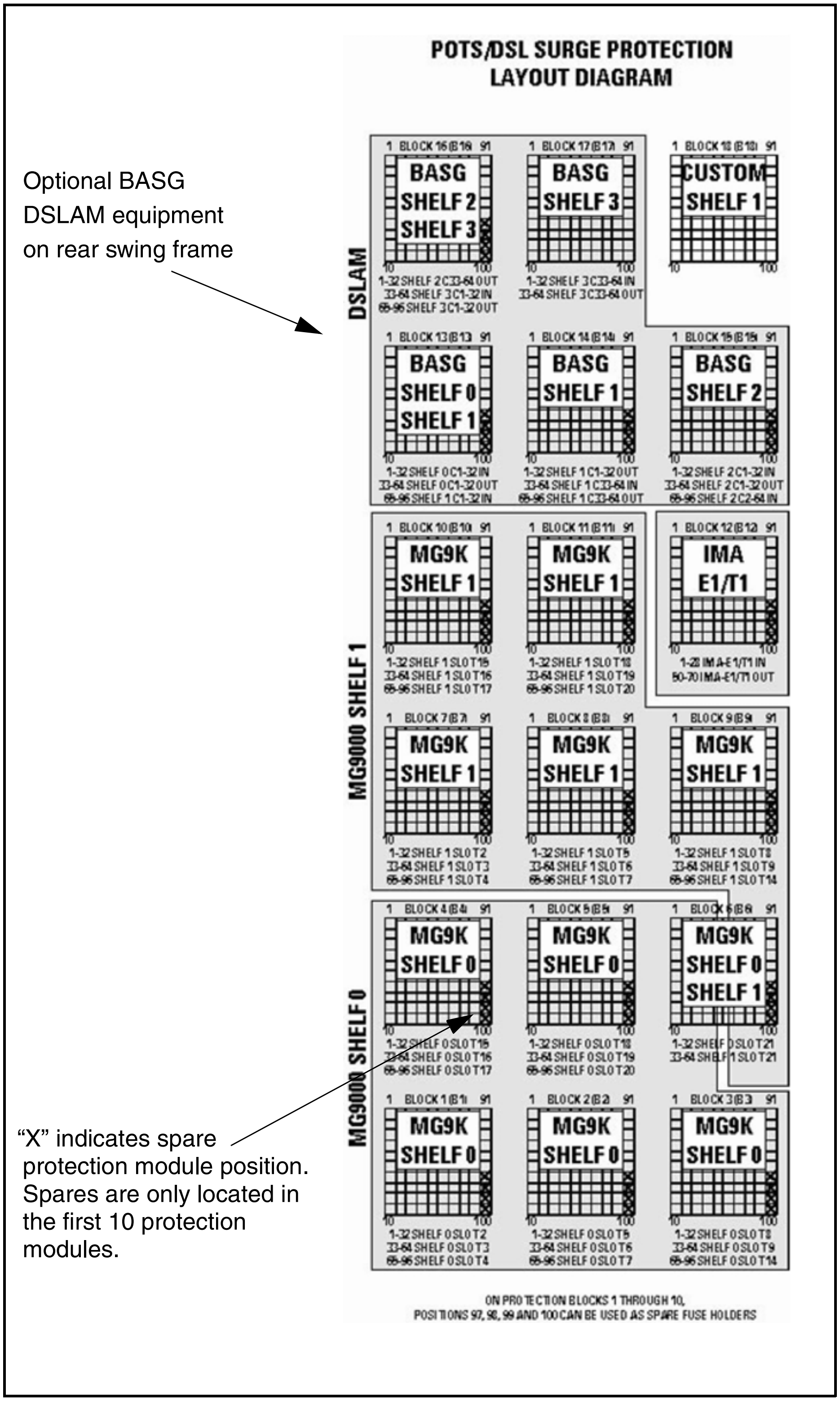
1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the service access compartment door.

2 Using the following diagram, which is the same as the diagram on the back of the door, locate the affected protection module to be replaced. The diagram maps each line card circuit to a protection module block. Identify the module based on the line with the fault connected to the line card in the MG 9000.

Obtain a spare protection module.

> ***Note:*** Spare 5-pin protection modules are stored in positions 97-100 on protection blocks 1-10.

Surge protection layout diagram



Optional BASG DSLAM equipment on rear swing frame

"X" indicates spare protection module position. Spares are only located in the first 10 protection modules.

3 Unplug the affected protector module.

4 Replace the protector module. Ensure the line card circuit fault clears.

5 Close and use a 3/8 in. nut driver to turn the door latch on the service access compartment door. Lock the door.

6 This procedure is complete.

Fuse replacement in the MG 9000 OPC

Purpose of this procedure

Use this procedure to replace fuses in the MG 9000 outside plant cabinet (OPC).

When to use this procedure

Perform this procedure as needed. When one of the OPC fuses has blown and needs replacement, an alarm appears at the Alarm Browser.

Action

Replacing a fuse in OPC

At the MG 9000 outside plant cabinet

1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front access door.

2 Perform a visual inspection of the fuses in the fuse panel at the top of the front bay.

- GMT fuses are located in to top row, in 5 A and 10 A ratings. A failed GMT fuse is identified by a colored button extending out the bottom from of the fuse.
- TPA fuses are located in the bottom row rated at 30 A.
A failed TPA fuse is identified by a red LED on the face of the fuse holder.

The following figure shows the fuse panel and fuse assignments. The placard in between the two sides identifies fuse assignment.

Fuse panel and fuse assignments

Side A

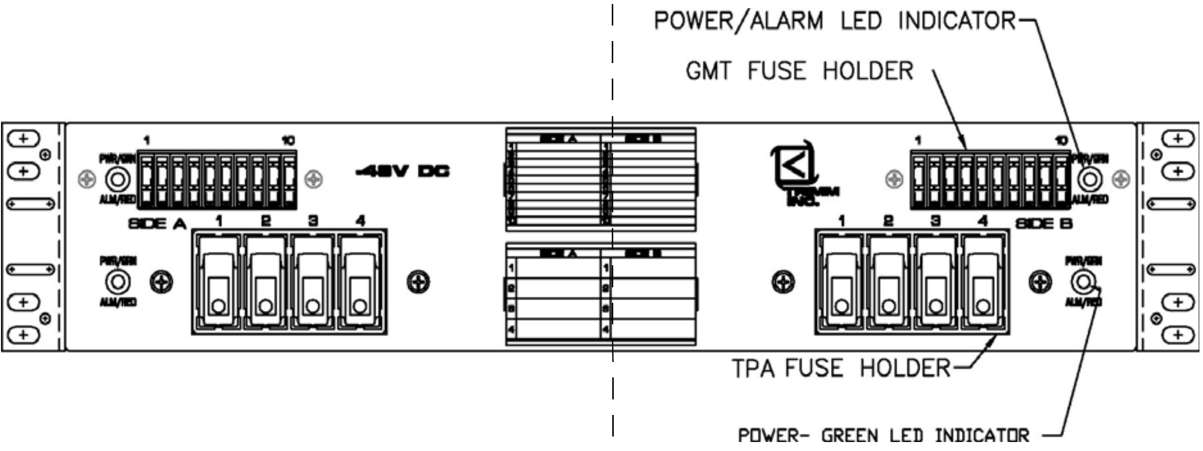
GMT

Fuse	Rating	Description
1		Not used
2		Not used
3		Not used
4		Not used
5		Not used
6		Not used
7		Not used
8		Not used
9		Not used
10		Not used

Side B

GMT

Fuse	Rating	Description
1	10 A	Heat exchanger
2		Not used
3	5 A	Fan Shelf - front fixed frame
4	5 A	IBIP ABS Power Supply
5		Not used
6		Not used
7	5 A	Not used
8	5 A	Not used
9	5 A	Not used
10	5 A	Not used



TPA

Fuse	Rating	Description
1	30 A	MG 9000 LA - 1 Feed
2	30 A	MG 9000 LTA - 1 Feed
3		Not used
4		Not used

TPA

Fuse	Rating	Description
1	30 A	MG 9000 LB - 1 Feed
2	30 A	MG 9000 LTB - 1 Feed
3		Not used
4		Not used

3 Replace the fuse with a fuse of the same rating. Spare fuses are located in the spare fuse mounting bracket located to the left side of the equipment bay on the upright. Ensure the TPA fuse is installed correctly, observing the placement of the orientation ring.

4 Close the access door and use a 3/8 in. nut driver to turn the door latch and lock the door.

5 This procedure is complete.

Replacing the fan tray in the MG 9000 OPC

Purpose of this procedure

Use this procedure to replace the NTM906MA fan tray in the front frame of an MG 9000 outside plant cabinet (OPC).

When to use this procedure

Perform this procedure when it is necessary to replace the NTM906MA fan tray because of faulty or failed fans.

Action

Replacing the NTM906MA fan tray in the OPC

At the MG 9000 outside plant cabinet site

1. Obtain a replacement NTM906MA fan tray
2. Unlock and use a 3/8 in. nut driver to turn the door latch and open the front and rear access doors.
3. From the rear access door, open the swing frame at the rear of the cabinet and disconnect the mate-lock connector on the rear of the fan tray. Clip the tie-wraps that secure the cable harness to the back of the fan tray.
4. From the front access door, use a 7 mm nut driver to remove the four M5 hex head screws that secure the fan tray.
5. Pull the fan tray to remove it from the frame.
6. Install the replacement fan tray and secure it in the frame using the four M5 hex head screws that were removed in step 4.
7. From the rear access door, connect the mate-lock connector to the rear of the fan tray. Tie-wrap the cable harness to the securing points on the back of the fan tray
8. Close the front and rear access doors. Use the 3/8 in. nut driver to latch the doors. Lock the doors.
9. Return the faulty fan tray for repair or replacement according to local procedures.
10. This procedure is complete.

Replacing the ac panel surge protector in the MG 9000 OPC

Purpose of this procedure

Use this procedure to replace the surge protector in an MG 9000 outside plant cabinet (OPC).

When to use this procedure

Perform this procedure when it is necessary to replace a failed surge protector in an MG 9000 outside plant cabinet. The surge protector has a red LED which lights when the surge protector has failed. In addition, a remote alarm will be sent to a scan point connected to the MG 9000 IBIP and raised at the MG 9000 Manager Alarm Browser.

Action

Replacing a surge protector in the OPC

At the MG 9000 outside plant cabinet site

1 Obtain a replacement surge protector, using Nortel Networks part number A0795133.

2 Unlock and use a 3/8 in. nut driver to turn the door latch and open the SAC door

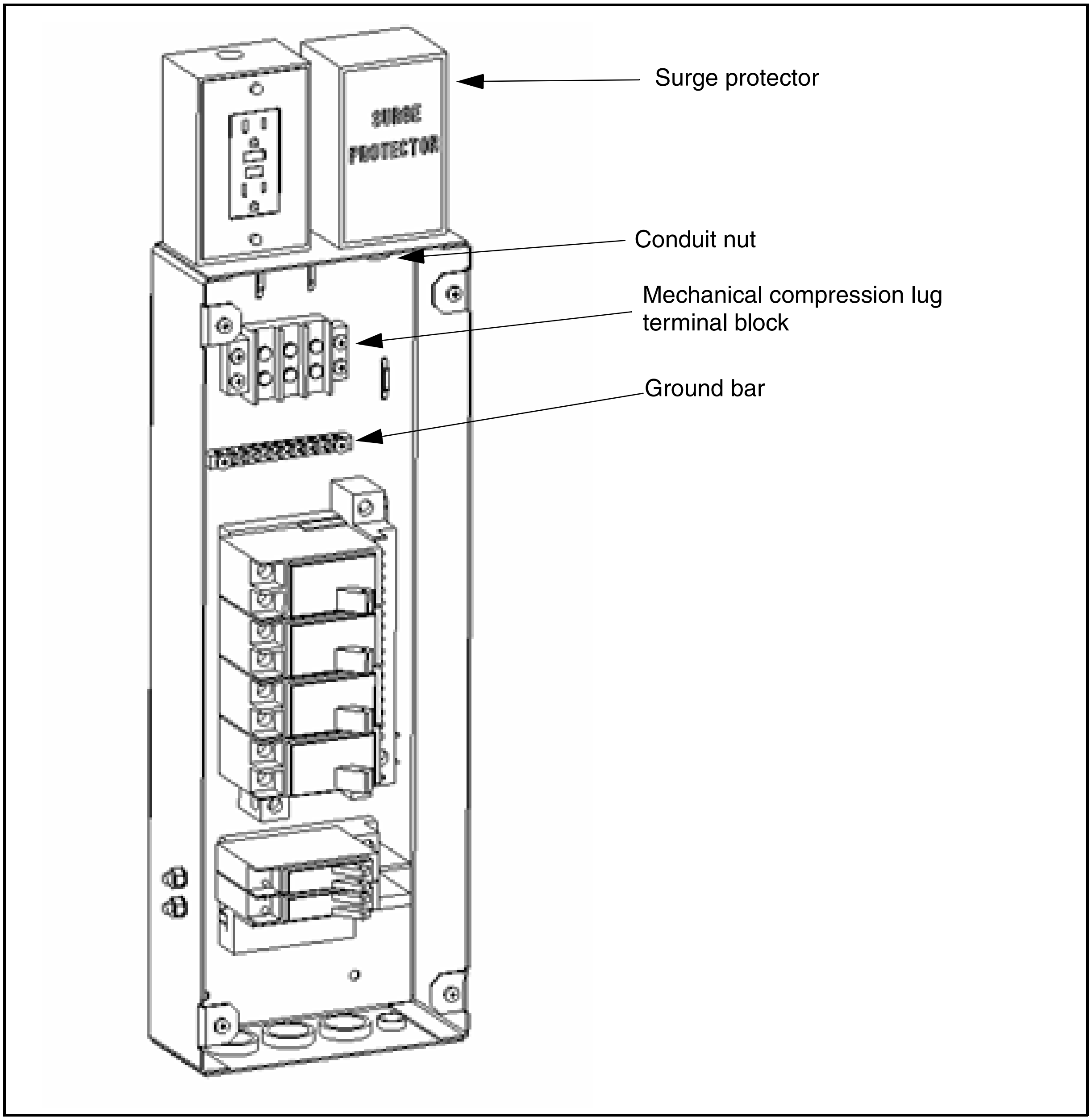
3

> **DANGER**
> **High voltages - live electrical circuits**
> The surge protector must be replaced without de-energizing the ac panel. This means the technician is exposed to high voltage 220 Vac circuits. Exercise extreme caution. Use insulated tools. Follow all safety procedures for your operating company when operating on live circuits.

Remove the six screws that secure the cover to the ac panel. Lay the cover aside.

Use the following figure to locate components in this procedure.

ac panel (cover removed) and surge protector



4 Remove the three leads (two hot, one neutral) that run to the surge protector from the mechanical compression lugs on the terminal block at the top of the ac panel. Label the wiring for proper installation.

5 Disconnect the surge protector ground wire from the ground bar.

6 Pull the wires free and out of the ac panel.

7 Label the alarm wiring. Loosen the two screws that secure the alarm wires on the alarm terminal block on the side of the Surge protector and release the wiring.

8 Loosen and remove the conduit locking nut that secures the surge protector to the top of the ac panel.

9 Carefully lift up the surge protector and pull it and the wires free of the ac panel.

10 Get the replacement surge protector and strip the wires 1/2 in. to bare the wires for installation.

11 Carefully route the new wires through the conduit into the ac panel.

12 Position the new surge protector to insert the conduit into the hole at the top of the ac panel.

13 Run the wiring through the conduit locking nut and screw the nut into place. Tighten the nut securely to prevent loosening because of vibration.

14 Connect the alarm wiring, noting the correct placement based on the labels applied in step 7.

15 Connect the ground wire to the ground bar.

16 Insert the three wires into the compression lugs on the terminal block at the top of the ac panel according to the label on the wires that were removed in step 4 and tighten the lugs.

17 Observe that the alarm clears on the Alarm Browser and that the red LED on the surge protector is not lit.

18 Set the ac panel cover in place and secure it with the six screws that were removed in step 3.

19 Close the service access cabinet door. Use the 3/8 in nut driver to latch the door. Lock the door.

20 This procedure is complete.

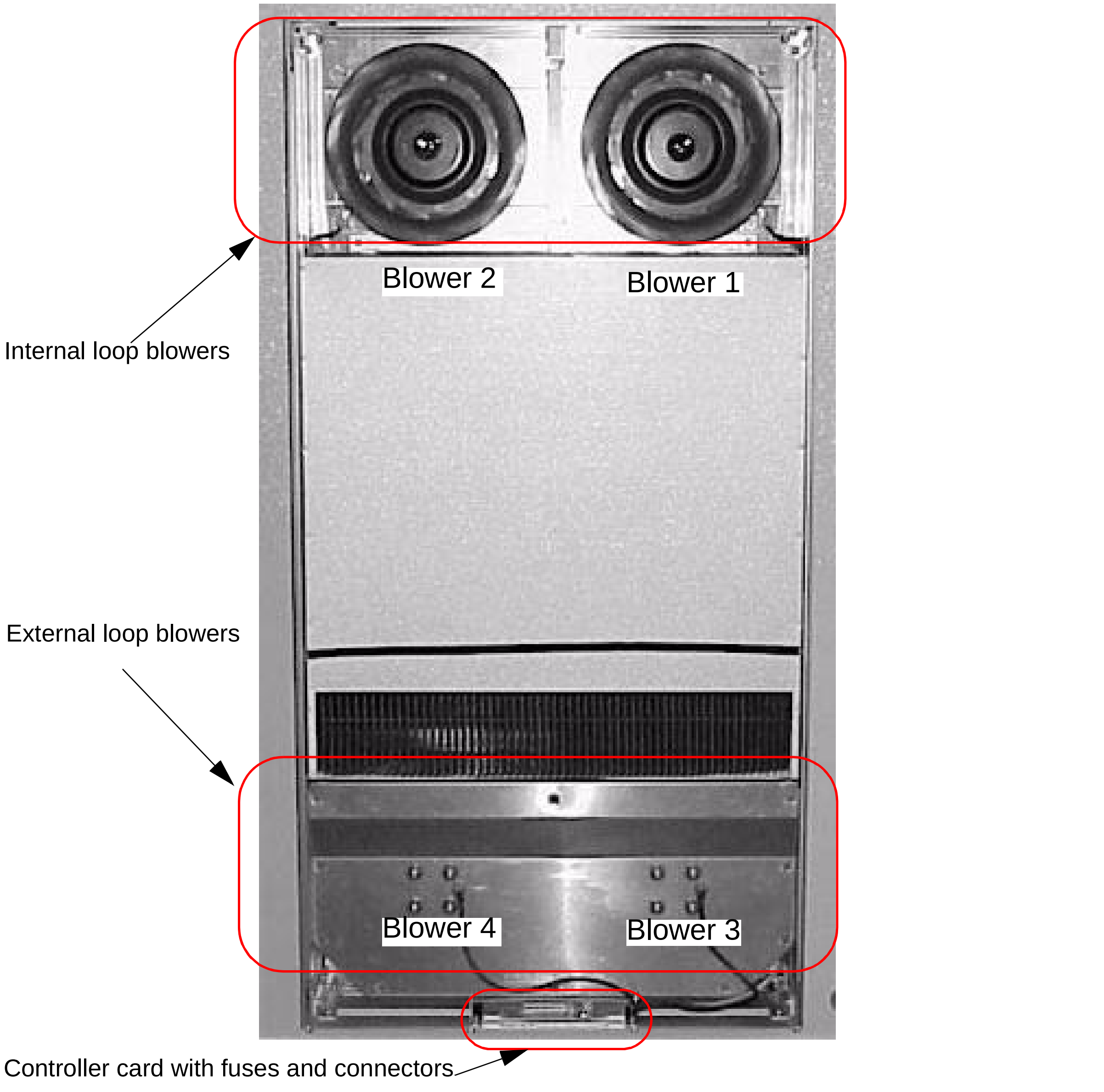
Replacing a heat exchanger blower in the MG 9000 OPC

Purpose of this procedure

Use this procedure to replace the heat exchanger blower in an MG 9000 outside plant cabinet (OPC).

The following figure shows the location of components referred to in this procedure.

Heat exchanger (shown with cover removed)



When to use this procedure

Perform this procedure when it is necessary to replace a heat exchanger blower because of faulty or failed blower unit.

Action

Replacing a heat exchanger blower in the OPC

At the MG 9000 outside plant cabinet site

1 Obtain a replacement heat exchanger blower and fuse. Use the following information to obtain the correct blower and fuse.

- internal loop blower (mounted on the top of the heat exchanger) - part number R1G220-AB73-76, Knurr no: 019140139
- external loop blower (mounted on the bottom of the heat exchanger) - part number R1G220-AB73-73 (with protected PCB), Knurr no: 019140129
- 3 A ceramic blower controller fuse - part number N0019048

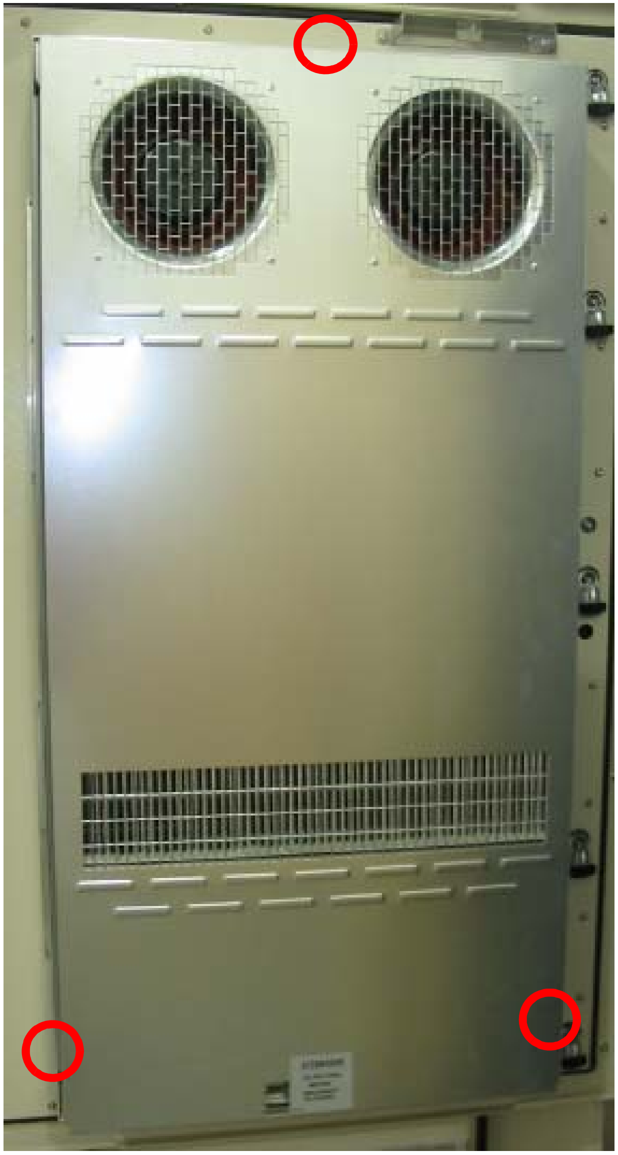
2 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front access door.

3 On the DC fuse panel in the front compartment, remove the 10A GMT fuse B1 to power down the heat exchanger blowers. Refer to figure Fuse panel and fuse assignments on page 445 to identify the fuse on the panel.

4 From the inside of the front access door, use a Phillips head screwdriver and remove the three Phillips head screws that secure the heat exchanger cover. There are three screws, one at the bottom left side edge, one at the bottom right side edge, and one screw at the top edge in the center of the heat exchanger.

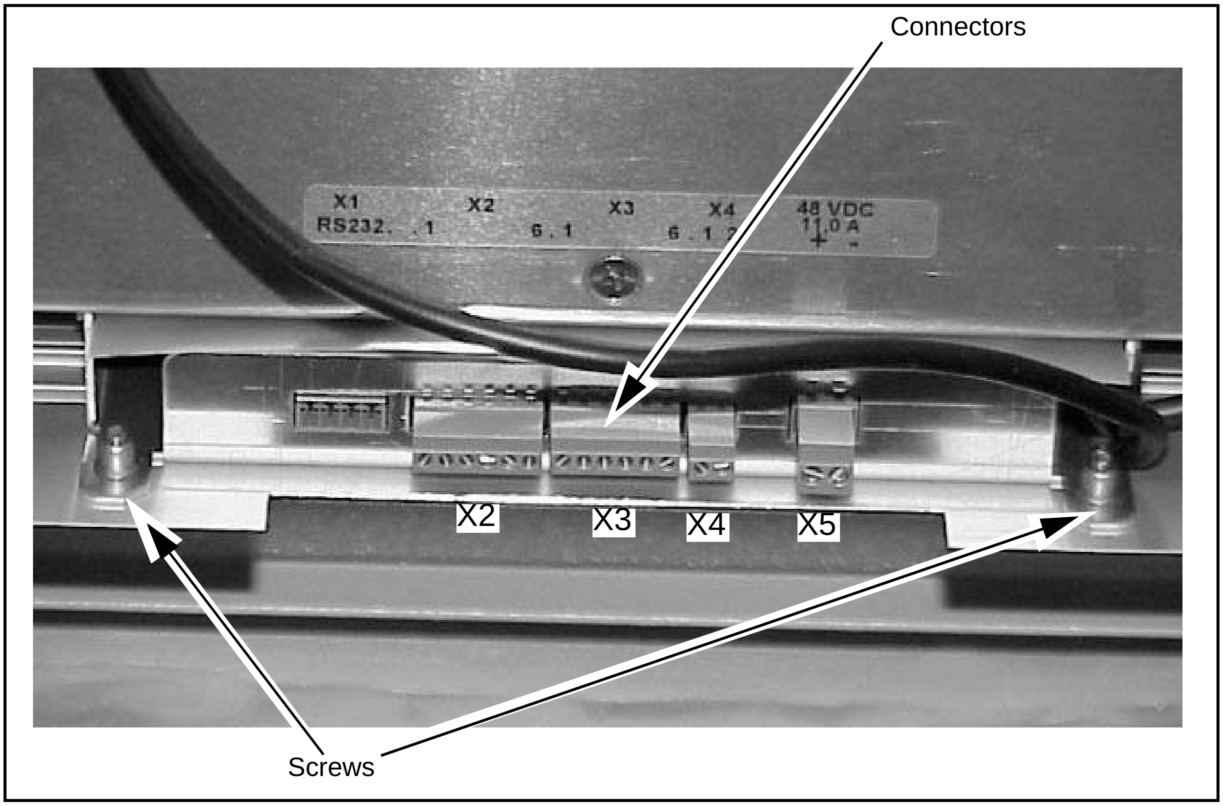
Use the following figure to locate the three screws.

Heat exchanger (identifying location of three cover screws)



5 Unplug connectors X2 through X5 on the controller board at the bottom of the heat exchanger cabinet. The following figure shows the controller card and the orientation of the connectors.

Heat exchanger controller card and connectors

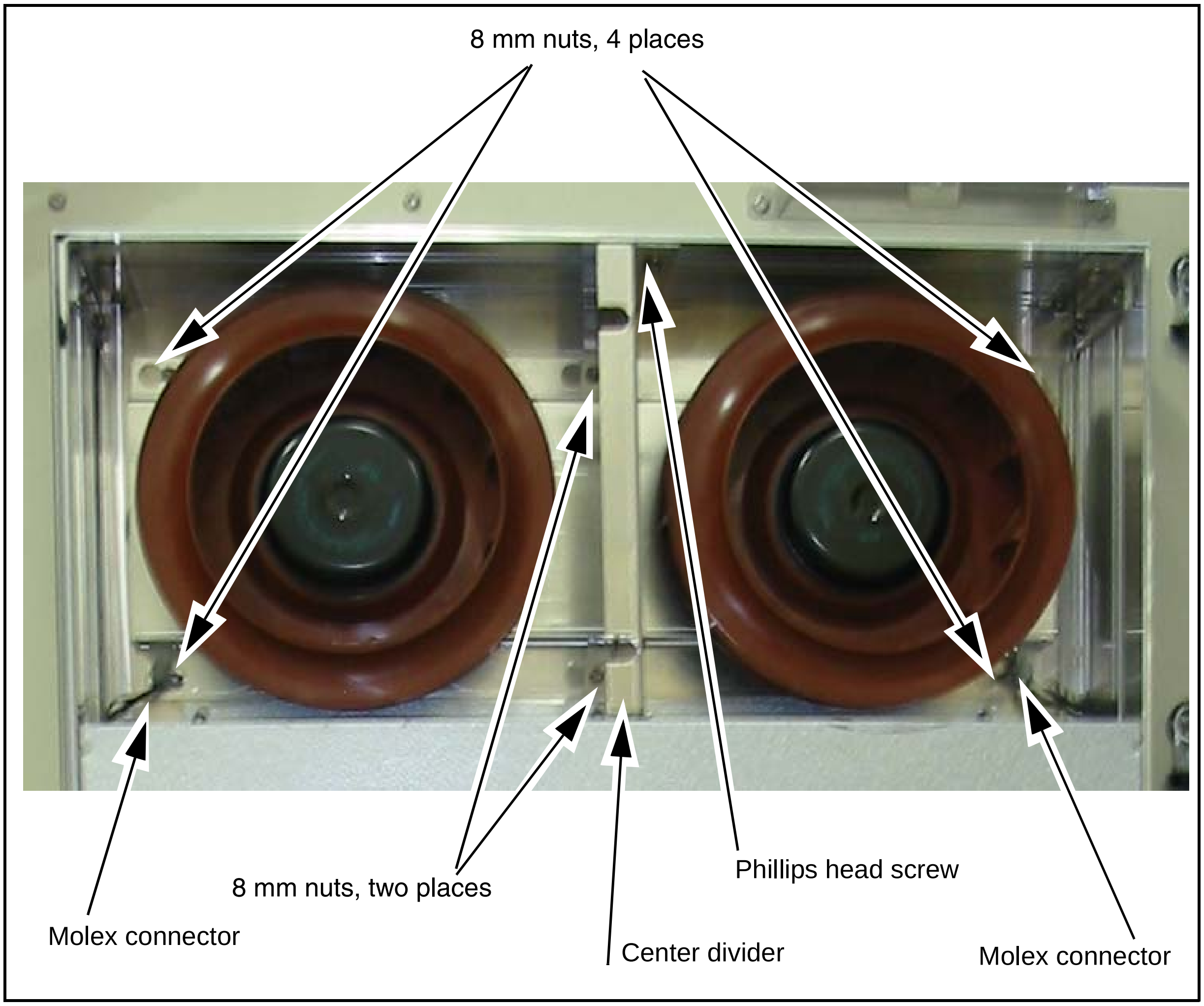


6 Use the information in the following table to determine the next step.

If replacing an	Do
internal loop blower	step 7
external loop blower	step 18

7 Use the following figure to identify the components in the steps for replacing an internal loop blower.

Internal loop blower compartment



8 Use an 8 mm nut driver to loosen the two nuts that secure the center divider in the internal loop blower compartment. On the right side of the divider, remove the Phillips head screw that secures the divider to the top of the heat exchanger cabinet. Slide the divider to the left and remove the divider.

9 Disconnect the two Molex connectors that supply power to the blowers, one at the bottom of each end of the internal loop blower compartment.

10 Use the 8 mm nut driver to loosen the four nuts, two at each end of the panel to which the blowers are mounted.

11 Slide the panel to the right and grasp the blower assembly and lift it clear of the cabinet.

12 Identify the faulty blower and turn the blower assembly over. Using a T25 Torx screwdriver, loosen and remove the four Torx

cap screws and rubber mounts that secure the blower to the panel. Remove the faulty blower.

13 Attach the replacement blower (part number R1G220-AB73-76, Knurr no: 019140139) and route the cable to the connector location. Attach the replacement blower to the panel using the Torx cap screws and rubber mounts. Tighten the cap screws using the T25 Torx screwdriver.

14 Set the panel back into the blower compartment, aligning the mounting holes with the mounting studs and nuts. Once properly aligned, slide the panel to the left.

15 Use the 8 mm nut driver to tighten the four nuts that were loosened in step 10.

16 Reconnect the Molex connectors that were disconnected in step 9.

17 Place the divider that was removed in step 7 into the compartment and slide it into position. Replace and tighten the Phillips head screw that was removed. Tighten the two 8 mm nuts to secure the divider to the panel.

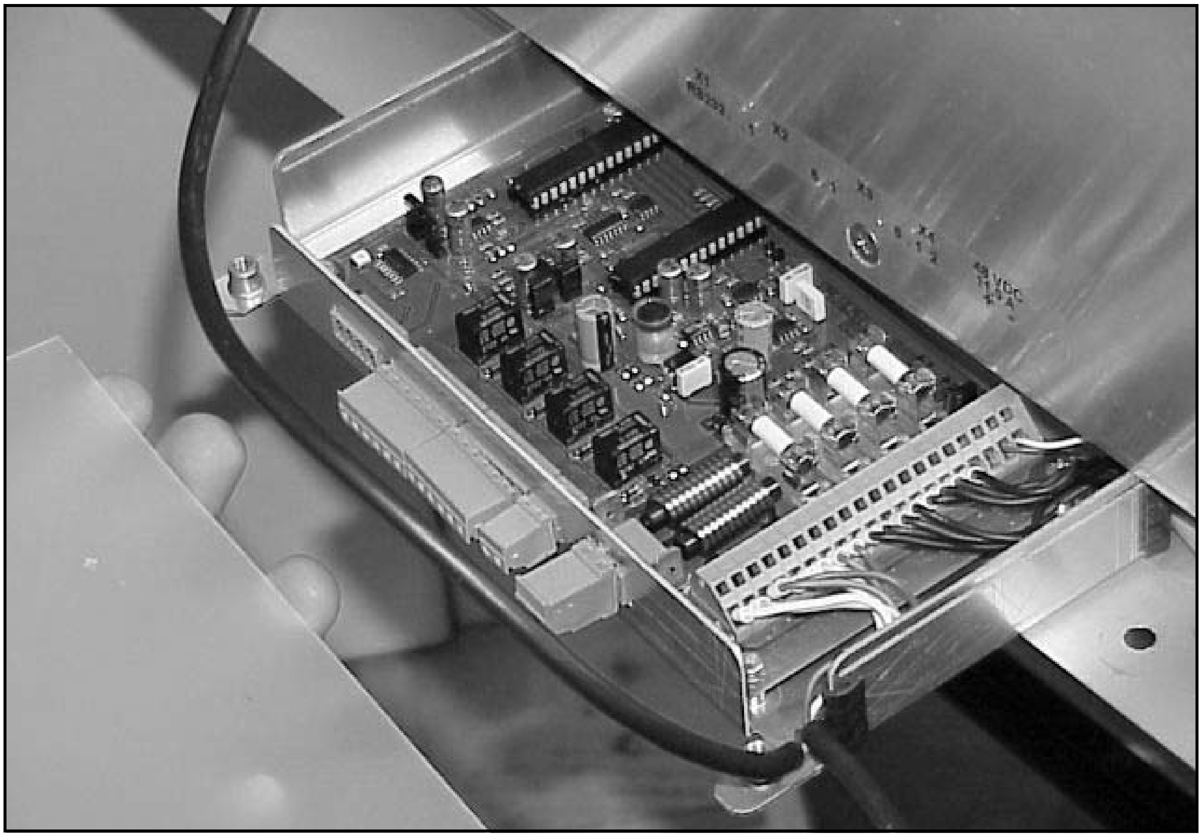
Go to step 34.

18 Pull the stiffener from the middle of the bottom edge of the heat exchanger, noting the placement of the small clips that hold the stiffener in place. Set the stiffener aside ensuring the clips are retrieved if they fall off.

19 From the bottom of the heat exchanger unit, unscrew the two Phillips head screws that hold the controller card in place as shown in the graphic in step 5.

20 Withdraw the controller card assembly from the heat exchanger. Gently remove the cover from the top of the assembly. The fuses and blower wiring connector are now exposed. The following figure shows the controller card, fuses, and wiring connector.

Heat exchanger blower controller card

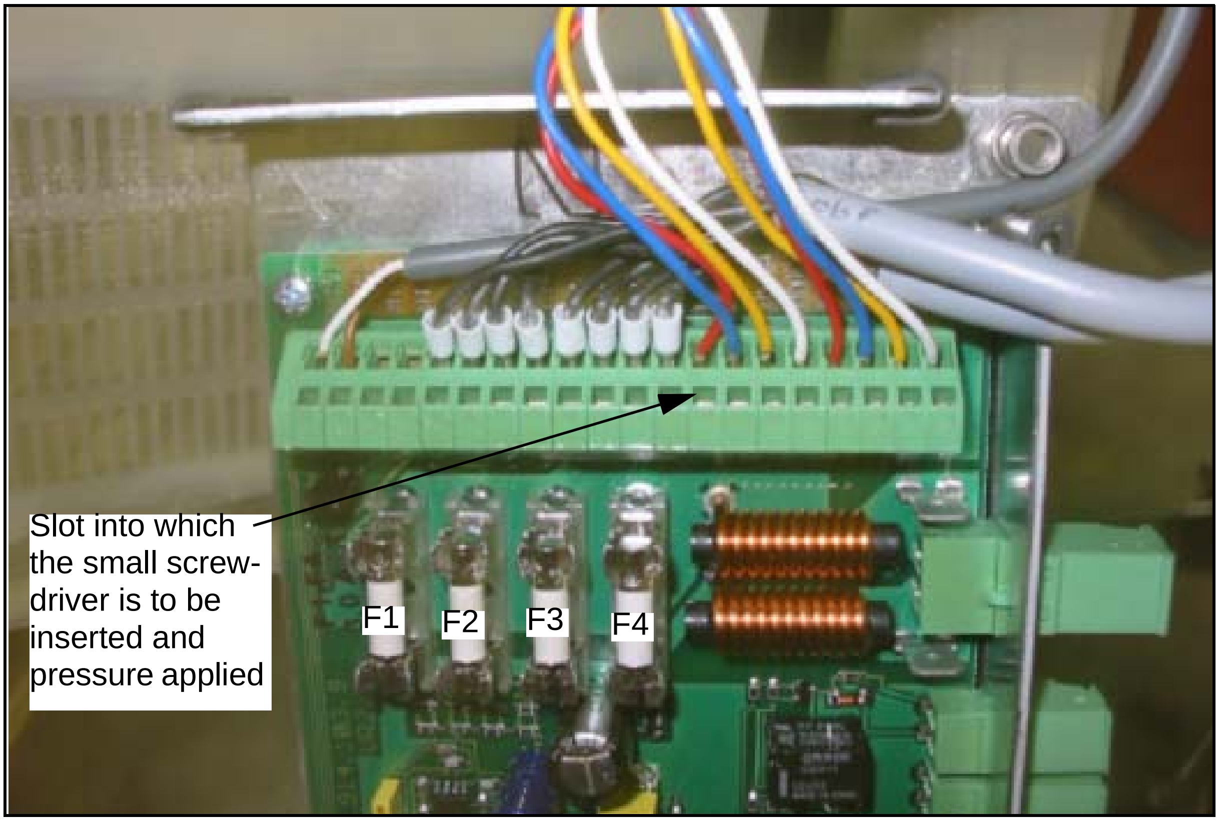


21 Identify the wires that feed the blower to be replaced. Label the wires and identify the specific slot in which they are connected to ensure proper connection with the new blower.

22 Four wires connect to each blower. Using a small flat blade screwdriver, press firmly into one of the slots adjacent to a wire that connects to the blower to be replaced. This action releases the wire. Repeat this action for all four wires.

The following figure shows the connector and the slot into which the screwdriver is to be inserted.

Controller card connector wiring and fuse labels


Slot into which the small screw-driver is to be inserted and pressure applied
F1
F2
F3
F4

23 Remove the ten Phillips head screws that secure the external loop blower panel to the heat exchanger unit.

24 Using a T25 Torx screwdriver, loosen and remove the four Torx cap screws and rubber mounts that secure the blower to the panel. Feed the wiring through the boot in the panel. Remove the faulty blower.

25 Route the wiring through the rubber boot. Attach the replacement blower (part number R1G220-AB73-73 (with protected PCB), Knurr no: 019140129) to the panel using the Torx cap screws and rubbers mounts. Tighten the cap screws using the T25 Torx screwdriver.

26 Set the external loop blower panel into the heat exchanger unit and secure it with the ten Phillips head screws that were removed in step 23.

27 Reconnect the four wires into the correct slots in the controller card connector based on how they were labeled on the old blower in step 21. Individually secure each wire into the appropriate slot using the screwdriver and same method to replace as was used to remove as described in step 22.

28 Replace the blown fuse that supplies the affected blower on the controller card with the correct fuse (part number N0019048). The fuses are labeled in figure Controller card connector wiring and fuse labels on page 458. The blowers are numbered as shown in figure Heat exchanger (shown with cover removed) on page 451. The relationship of fuse to blower is as follows:

- Fuse F1 - Blower 1 on top right
- Fuse F2- Blower 2 on top left
- Fuse F3 - Blower 3 on bottom right
- Fuse F4- Blower 4 on bottom left

29 Gently replace the controller card cover onto the top of the assembly. Insert the controller card assembly into the heat exchanger.

30 From the bottom of the heat exchanger unit, replace the two Phillips head screws that secure the controller card. Tighten the screws.

31 Replace the stiffener onto the middle of the bottom edge of the heat exchanger, noting the placement of the small clips that hold the stiffener in place.

32 Reconnect connectors X2 through X5 that were disconnected in step 5.

33 On the DC fuse panel in the front compartment, replace GMT fuse B1 to power up the heat exchanger blowers. Ensure proper operation of the heat exchanger and that any alarm related to the faulty blower has now cleared.

34 Replace the heat exchanger cover and the three Phillips head screws that were removed in step 4.

35 Close the front access door. Use the 3/8 in. nut driver to latch the door. Lock the door.

36 This procedure is complete.

Removing dust from the MG 9000 OPC

Purpose of this procedure

Use this procedure to remove dust in an MG 9000 outside plant cabinet (OPC).

When to use this procedure

Perform this procedure every six months or according to local procedure.

Requirements

A vacuum cleaner with an induction-wound brushless motor and plastic or rubber attachment must be used to prevent electromagnetic interference.

Action

Removing dust from OPC

At the MG 9000 outside plant cabinet site

1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front access, rear access door, and SAC doors.

2 Vacuum the outside plant frames to prevent the increase of electrostatic discharges that accompany dust buildup. Use a vacuum cleaner with an induction-wound brushless motor and plastic or rubber attachments. A battery-operated vacuum cleaner can be used. Vacuum inside and around the frames. Do not bump any part of the frame. Avoid metal-to-metal contact.

3 Close the front, rear, and SAC doors. Use the 3/8 in nut driver to latch the doors. Lock the doors.

4 This procedure is complete.

Cleaning and testing the fans in the MG 9000 OPC

Purpose of this procedure

Use this procedure to clean and test the fans in an MG 9000 outside plant cabinet (OPC).

When to use this procedure

Perform this procedure when local policy directs.

Action

Cleaning and testing fans in OPC

At the MG 9000 outside plant cabinet site

1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front access, rear access, and SAC doors.

2 To de-energize the heat exchanger on the front door, pull fuse B1 for the heat exchanger on the fuse panel at the top of the main frame. Refer to the figure showing the Fuse panel and fuse assignments on page 445 to correctly identify the fuse.

3 Remove the three Phillips head screws that secure the heat exchanger cover in place to the inside of the front access door. Lift up on the heat exchanger cover to expose the heat exchanger and fans. Clean the fan blades. Manually rotate the fans to check for smooth operation of the fans.

4 Use the information in the following table to determine the next step.

If fan blades	Do
turn smoothly	step 5
do not turn smoothly	Replace the faulty fan and return to this step.

5 Install the heat exchanger cover. Secure the cover with the three Phillips head screws that were removed in step 3.

6 Replace the fuse removed in step 2.

7 Open the swing frame at the rear of the cabinet and disconnect the Mate-N-Lok connector on the rear of the fan tray in the front frame.

8 From the front access, use a 7 mm nut driver to remove the four M5 hex head screws that secure the fan tray.

9 Pull the fan tray to remove it from the frame.

10 Clean the fan blades. Manually rotate the fans to check for smooth operation of the fans.

If fan blades	Do
turn smoothly	step 11
do not turn smoothly	step 14

11 Install the fan tray and secure it in the frame using the four M5 hex head screws that were removed in step 8.

12 Reconnect the Mate-N-Lok connector to the rear of the fan tray. If the fans are not operating when power is returned, use a heat gun or blow dryer on the fan thermostat sensor to turn on the fans. Again observe the fans for correct and smooth operation.

If the fans are	Do
operating correctly	step 15
not running, running roughly, or not operating correctly	step 14

13 If a fan tray is installed in the swing frame at the rear of the cabinet, repeat steps 8 through 12.

14 Replace the fan tray using the procedure Replacing the NTM906MA fan tray in the OPC on page 446. Go to step 16.

15 Close the front, rear, and SAC cabinet doors. Use the 3/8 in. nut driver to latch the doors. Lock the doors.

16 This procedure is complete.

Battery inspection and cleaning in the MG 9000 OPC

Purpose of this procedure

Use this procedure to inspect and clean the batteries in an MG 9000 outside plant cabinet (OPC).

When to use this procedure

Perform this procedure every six months or according to local procedures.

Action

Inspecting and cleaning batteries in OPC

At the MG 9000 outside plant cabinet site

1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front access door.

2 Use a T25 Torx driver, loosing the three Torx screws to open the rear battery access rear door.

3

> **DANGER**
> **Hazardous chemicals**
> Battery chemical can be dangerous and potentially explosive. Exercise caution.

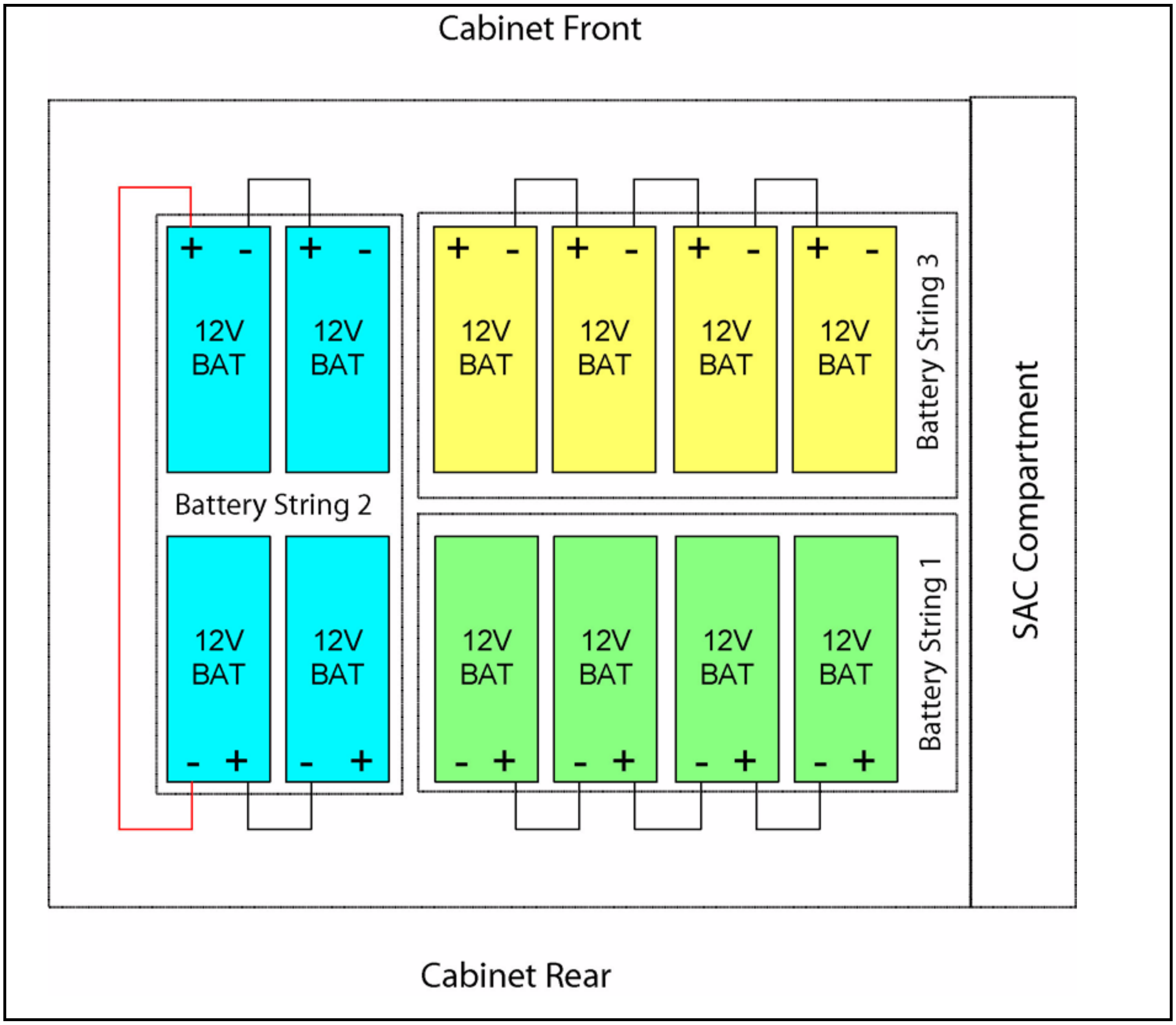
Inspect battery packs, connections, and floor for moisture or corrosion.

4 Use the following table to determine the next step.

If moisture or corrosion	Do
is present	step 5
is not present	step 13

5 Identify the affected string(s). Use the following figure to identify the battery strings.

Battery arrangement in the outside plant cabinet



6

CAUTION
Possible loss of service during battery replacement.
Do not disconnect more than one battery string at a time. If more than one battery string is turned off at a time and ac power is interrupted, service may be interrupted.

Open the SAC door and set the affected battery string to off on the battery disconnect panel, located at the top right of the SAC compartment.

7 Disconnect and remove the affected battery string from the affected area.

8 Clean the affected area with baking soda and water. Continue until the cleaning solution does not foam when the cleaning solution is applied.

9 Dry the cleaned area completely and replace the batteries.

10 Reconnect the battery string.

11 In the SAC compartment, set the breaker for the de-energized battery string to the On position.

12 Use the information in the following table to determine the next step.

If	Do
all moisture or corrosion has been removed	step 13
additional moisture or corrosion is noted on other battery strings	repeat steps 5 through 11

13 Close the battery compartment access door and use the T25 Torx driver to tighten the three Torx screws.

14 Close the front cabinet door. Use the 3/8 in nut driver to latch the door. Lock the door.

15 This procedure is complete.

GFCI check in the MG 9000 OPC

Purpose of this procedure

Use this procedure to ensure the ground fault circuit interrupt (GFCI) for the outside plant cabinet (OPC) operates correctly.

When to use this procedure

Perform this procedure before using the GFCI outlet in the OPC.

Action

Performing a GFCI check in OPC

At the MG 9000 outside plant cabinet

1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the SAC door.

2 Press the test button the GFCI outlet.

3 Verify that the Reset button pops out.

If the Reset button	Do
pops out	step 4
does not pop out	step 5

4 Press the Reset button.

If the Reset button	Do
does not stay pressed	step 5
stays pressed	step 6

5 For additional help, contact the next level of support.

6 Close the service access compartment door. Use the 3/8 in nut driver to latch the door. Lock the door.

7 This procedure is complete.

Performing a ground check in the MG 9000 OPC

Purpose of this procedure

Use this procedure to perform a check of the MG 9000 outside plant cabinet (OPC) ground connection and measure ground resistance.

When to use this procedure

Perform this procedure according to local policy.

Action

Performing a ground check in OPC

At the MG 9000 outside plant cabinet site

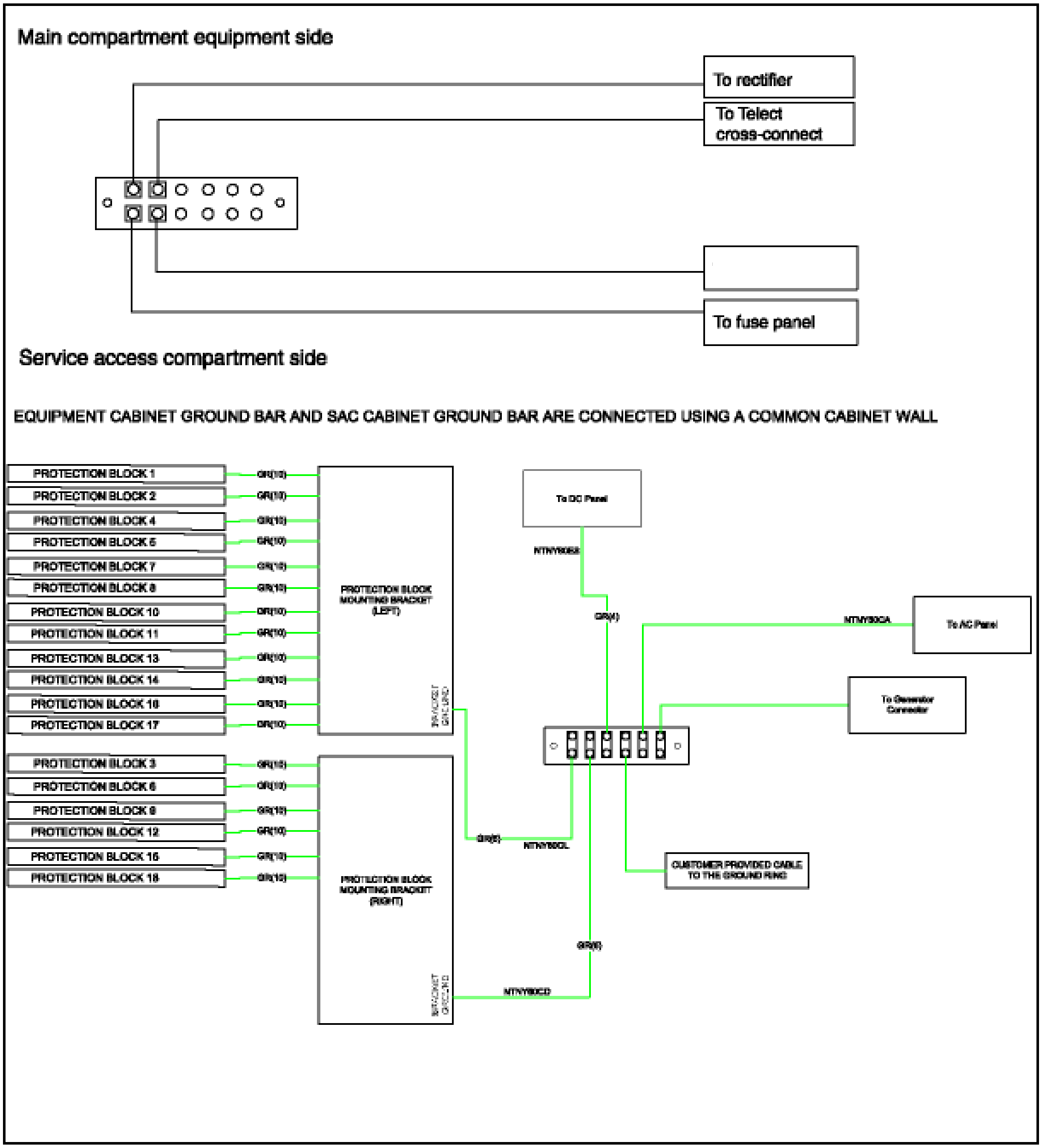
1 Unlock and use a 3/8 in. nut driver to turn the door latch and open the front and SAC doors.

2 Check the system grounds.

If grounds	Do
are in good condition	step 4
are damaged	step 5

3 Refer to the following figure to identify system grounds.

Outside plant cabinet system ground points



4 Use local approved methods to measure ground resistance. The resistance for each ground must be ≤ 25 Ohms.

If the resistance is	Do
≤ 25 Ohms	step 6

If the resistance is	Do
≥ 25 Ohms	step 5

5 For additional help, contact the next level of support.

6 Close the front and SAC doors. Use the 3/8 in nut driver to latch the door. Lock the doors.

7 This procedure is complete.

Testing wrist strap grounding cords in the MG 9000 OPC

Purpose of this procedure

Use this procedure to test the resistance of the wrist strap grounding cords. Check that the resistance is low enough to allow static electricity to discharge from the body of the user. Resistance must be high enough to prevent electrocution of the user if the equipment develops a short.

When to use this procedure

Perform this procedure once each month or according to local procedures.

Action

Wrist strap grounding cords test

At the MG 9000 outside plant cabinet

1 Remove the grounding cord from the wrist strap.

2

DANGER
Risk of Electrocution
The grounding cord is safe to use only if the resistance of the cord measures higher than 800 kilohms. A lower resistance can cause electrocution if equipment short-circuits while the user wears the wrist strap.

WARNING
Damage to electronic equipment
A grounding cord that has a resistance higher than 1200 kilohms cannot conduct static charges to ground correctly. This cord does not protect sensitive electronic equipment against build-ups of charges that can damage the equipment.

Measure the resistance between opposite ends of the grounding cord with an ohmmeter.

If resistance	Do
is between 800 kilohms and 1200 kilohms	step 5
is not between 800 kilohms and 1200 kilohms	step 3

3 Remove the whole assembly. Do not attempt to use the assembly.

4 Replace the assembly as soon as possible. Go to step 1 for new assembly.

5 You can use the grounding cord and wrist strap assembly. Assemble the wrist strap to the grounding cord.

6 This procedure is complete.